



Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

FREEDOM OF INFORMATION ACT PROGRAM

April 20, 2020

In reply refer to: FOIA #BPA-2020-00547-F

Kartikay Mehrotra
Bloomberg News
Pier 3 Suite 201
San Francisco, CA 94111
Email: kmehrotra2@bloomberg.net

Dear Mr. Mehrotra,

Thank you for your interest in the Bonneville Power Administration (BPA). The agency received your request for records made under the Freedom of Information Act, 5 U.S.C. § 552, (FOIA). Your request was received on February 28, 2020, and was formally acknowledged on March 5, 2020. The agency's final response to your FOIA request follows.

Request

“...the following documents (“the Records”): Correspondence regarding Sen. Ed Markey’s request: 1.) Documents: Name: Any document created by the BPA Office of Cyber Security with "Electric Utility Attacks Letters to Federal Power Marketing Orgs" in the title to include drafts used for input Date: Between September 2018 and October 2018 2.) Emails: Any email that includes the subject: Signed - Markey letter re Cyber Attacks.pdf Dates: Between September 2018 and October 2018 Red Team Remediation: 3.) Emails: Any email by the BPA Office of Cyber Security that includes information regarding the most recent remediation status of the vulnerabilities or weaknesses determined by the BPA Red Team report. Date: 10/3/2017 4.) Subject: "CCN Red Team (TO) POAM Remediation Status for the Week Ending November 10, 2017" From: Alicia Collier 5.) Documents: Any documents created by the BPA Office of Cyber Security [that] includes the most recent remediation status of the vulnerabilities or weaknesses determined by the BPA Red Team report. Dates: Between January 2020 to present 7.) Documents: Name: "Red Team Vulnerability Remediation Completion Report" Location: Cyber Security file share Dates: 3/2015 - 10/2015[.] This request is ongoing, seeking copies of (or access to) all Records as they are filed with the Bonneville Power Administration.”

Amendment

BPA notified you on March 5, 2020, that the following section of your request does not fulfill the criteria of a proper request under the FOIA and the applicable DOE regulations: “...This request is ongoing, seeking copies of (or access to) all Records as they are filed with the Bonneville Power Administration.” The FOIA does not provide an avenue for a requester to obtain agency records not already existing. BPA accepted that portion of your request with the

following alteration: “[all responsive records dated] through February 28, 2020 [the date your request was received by BPA].”

Response

The agency searched for and located 250 pages of records responsive to your request. BPA is herein releasing all pages, with certain pages containing minimal redactions applied as follows:

- Nine redaction made under 5 U.S.C. § 552(b)(2) (Exemption 2)
- 16 redactions made under 5 U.S.C. § 552(b)(5) (Exemption 5)
- Six redactions made under 5 U.S.C. § 552(b)(6) (Exemption 6)

Exemptions

The FOIA generally requires the release of all responsive agency records upon request. However, the FOIA permits or requires withholding certain limited information that falls under one or more of nine statutory exemptions (5 U.S.C. §§ 552(b)(1-9)).

Exemption 2

Exemption 2 protects information related to the internal personnel rules and practices of an agency. BPA has applied limited Exemption 2 redactions to protect internal call-in numbers, pass codes for recurring agency meetings, and file paths for agency files. BPA has considered and declined a discretionary release of that information because disclosure would harm the interests protected and encouraged by Exemption 2.

Exemption 5

Exemption 5 serves to protect records showing the deliberative or decision-making processes of government agencies. Records protected under Exemption 5 must be both pre-decisional and deliberative. A record is pre-decisional if it is generated before the adoption of an agency policy; a record is deliberative if it reflects the give-and-take of the consultative process, either by assessing the merits of a particular viewpoint or by articulating the process used by the agency to formulate a decision. BPA relies on Exemption 5 to protect BPA Cyber Security staff viewpoints and recommendations expressed in the responsive records. BPA has considered and declined a discretionary release of that pre-decisional and deliberative information because disclosure would harm the interests encouraged and protected by Exemption 5.

Exemption 6

Exemption 6 protects personally identifiable information (PII) when the disclosure of such information would constitute a clearly unwarranted invasion of personal privacy, provided there is no public interest that outweighs the privacy interest. BPA relies on Exemption 6 to withhold employee mobile telephone numbers and employee leave information. BPA can find no public interest in disclosing this information as it does not shed light on the BPA's operation as an agency. The privacy interest protected by Exemption 6 belongs to the individual and therefore BPA cannot discretionarily release that information.

Fees

There are no fees associated with the response to your request.

Certification

Your FOIA request BPA-2020-00547-F is now closed with all available agency records provided. Pursuant to 10 C.F.R. § 1004.7(b) (2), I am the individual responsible for the records search, exemption determinations and records release described above.

Appeal

The adequacy of the search may be appealed within 90 calendar days from your receipt of this letter pursuant to 10 C.F.R. § 1004.8. Appeals should be addressed to:

Director, Office of Hearings and Appeals
HG-1, L'Enfant Plaza
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585-1615

The written appeal, including the envelope, must clearly indicate that a FOIA appeal is being made. You may also submit your appeal by e-mail to OHA.filings@hq.doe.gov, including the phrase "Freedom of Information Appeal" in the subject line. (The Office of Hearings and Appeals prefers to receive appeals by email.) The appeal must contain all the elements required by 10 C.F.R. § 1004.8, including a copy of the determination letter. Thereafter, judicial review will be available to you in the Federal District Court either (1) in the district where you reside, (2) where you have your principal place of business, (3) where DOE's records are situated, or (4) in the District of Columbia.

You may contact BPA's FOIA Public Liaison, Jason Taylor, at 503-230-3537, jetaylor@bpa.gov, or the address on this letter header for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road-OGIS
College Park, Maryland 20740-6001
E-mail: ogis@nara.gov
Phone: 202-741-5770
Toll-free: 1-877-684-6448
Fax: 202-741-5769

Thank you again for your interest in the Bonneville Power Administration.

Sincerely,



Candice D. Palen, Freedom of Information/Privacy Act Officer

EDWARD J. MARKEY
MASSACHUSETTS

Sum SD--255
DIR ICSEN 8 U1LD 1NG
WASHINGTON, OC 20510-2107
202- 224-2742

tnitrd mtcs rnate

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, Sun< 312
FALL RIVER, MA 02 721
508-677-0523

1550MAIN STAFET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

COMMITTEES :
ENVIRONMENT AND PUBLIC WORKS
FOREIGN RELATIONS
RANKING MEMBER:
SOUTH CHINA AND EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY
COMMERCE, SCIENCE, AND TRANSPORTATION
RANKING MEMBER:
SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS
SMALL BUSINESS AND ENTREPRENEURSHIP
CHAIRMAN:
U.S. SENATE CLIMATE CHANGE TASK FORCE

August 13, 2018

Elliot Mainzer, Administrator
Bonneville Power Administration
P.O. 3621
Portland, OR 97208

Dear Mr. Mainzer,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how you are working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third-party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors - companies "who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order."³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (OHS) considered the threat of cyberattack so serious that it issued an alert warning industry and government officials about it.⁵ That same year, I released a report entitled "Electric Grid

¹Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

²*Id.*

³*Id.*

⁴*Id.*

⁵Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

Vulnerability: Industry Responses Reveal Security Gaps," which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled "Cyber Threat and Vulnerability Analysis of the U.S. Electric Center," which warned that, "[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication."⁷ And just last year, in the Department of Energy's Quadrennial Energy Review, that agency found that the "cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures" and recommended that "system planning must evolve to meet the need for rapid response to system disturbances."⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.
2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

⁶ Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.13.L.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

⁸ Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

⁹ 83 FR 17913

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?
4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.
5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.
6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?
7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

COMMITTEES:
ENVIRONMENT AND PUBLICWORKS

FORIGN RELATIONS

RANKING MEMBER

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

Subcommittee on

SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN

U.S. SENATE CLIMATE CHANGE TASK FORCE

tinitro tats rnatr

97 5 JF K FEOR RAI BUIIDIN<,
15 NEW SU DBURY STREET
BOSTON, MA 02203
617-5 65-<1519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-6 77-0 523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

August 13, 2018

David Rousseau, President
Salt River Project
1500 N. Mill Ave.
Tempe, AZ 85281

Dear Mr. Rousseau,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how you are working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third-party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors - companies "who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order."³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (OHS) considered the threat of cyberattack so serious that it issued an alert warning industry and government officials about it.⁵ That same year, I released a report entitled "Electric Grid

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/worId/na t iona l-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story .htm l

Vulnerability: Industry Responses Reveal Security Gaps," which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled "Cyber Threat and Vulnerability Analysis of the U.S. Electric Center," which warned that, "[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication."⁷ And just last year, in the Department of Energy's Quadrennial Energy Review, that agency found that the "cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures" and recommended that "system planning must evolve to meet the need for rapid response to system disturbances."⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.
2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

⁶Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016),

<https://www.energy.gov/sites/prod/files/2017/02/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

⁸Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017),

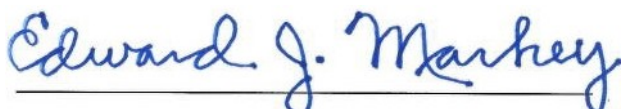
<https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

⁹83 FR 17913

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?
4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.
5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.
6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?
7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON

SPACE, SCIENCE, AND COMPLETION

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

August 13, 2018

Mr. Kenneth Legg, Administrator
Southeastern Power Administration
1166 Athens Tech Rd.
Elberton, GA 30635

Dear Mr. Legg,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how you are working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third-party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors - companies "who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order."³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (DHS) considered the threat of cyberattack so serious that it issued an alert warning industry and government officials about it.⁵ That same year, I released a report entitled "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps," which found that the electric grid was

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security--officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled "Cyber Threat and Vulnerability Analysis of the U.S. Electric Center," which warned that, "[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication."⁷ And just last year, in the Department of Energy's Quadrennial Energy Review, that agency found that the "cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures" and recommended that "system planning must evolve to meet the need for rapid response to system disturbances."⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.
2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

"Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/t34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

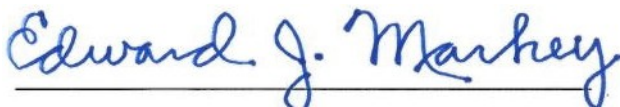
⁸ Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/t34/Quadrennial%20Energy%20Review--Second%20Installment%20-%28%20Full%20Report%29.pdf>

⁹ 83 FR 17913

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?
4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.
5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.
6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?
7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,



Edward J. Markey

United States Senator

EDWARD J. MARKEY
MASSACHUSETTS

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 N EW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-(77-0523

1550 MA N STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

tinittd tatr rnatc

COMMITTEES:
ENVIRONMENTAL AND PUBLIC WORKS
FOREIGN RELATIONS
RANKING MEMBER:
SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL COOPERATION AND SECURITY POLICY
COMMERCE, SCIENCE, AND TRANSPORTATION
RANKING MEMBER:
SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS
SMALL BUSINESS AND ENTREPRENEURSHIP
CHAIRMAN:
U.S. SENATE CLIMATE CHANGE TASK FORCE

August 13, 2018

Mike Wech, Administrator
U.S. Department of Energy
Southwestern Power Administration
Room 8G-027/ Forrestal
1000 Independence Avenue, SW
Washington, DC 20585

Dear Mr. Wech,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how you are working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third-party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors - companies "who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order."³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (OHS) considered the threat of cyberattack so serious that it issued an alert warning industry and

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

government officials about it.⁵ That same year, I released a report entitled "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps," which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled "Cyber Threat and Vulnerability Analysis of the U.S. Electric Center," which warned that, "[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication."⁷ And just last year, in the Department of Energy's Quadrennial Energy Review, that agency found that the "cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures" and recommended that "system planning must evolve to meet the need for rapid response to system disturbances."⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.
2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party

⁵Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

⁶Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016),

<https://www.energy.gov/sites/prod/files/2017/01/t34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.%20Electric%20Sector.pdf>

⁸Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017),

<https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

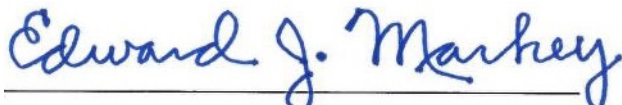
⁹83 FR 17913

firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?
4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice,(b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.
5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.
6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?
7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

EDWARD J. MARKEY
MASSACHUSETTS

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDAV STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STACO, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

tlnitro tats rnetc

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS
FOREIGN RELATIONS
RANKING MEMBER:
SUBCOMMITTEE ON EAST ASIA, PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY
COMMERCE, SCIENCE, AND TRANSPORTATION
RANKING MEMBER:
SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS
SMALL BUSINESS AND ENTREPRENEURSHIP
CHAIRMAN:
SENATE CLIMATE CHANGE TASK FORCE

August 13, 2018

William D. Johnson, President and CEO
Tennessee Valley Authority
400 West Summit Hill Drive
Knoxville, TN 37902

Dear Mr. Johnson,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how you are working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third-party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors - companies "who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order."³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (DHS) considered the threat of cyberattack so serious that it issued an alert warning industry and government officials about it.⁵ That same year, I released a report entitled "Electric Grid

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/u-swams-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

Vulnerability: Industry Responses Reveal Security Gaps," which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled "Cyber Threat and Vulnerability Analysis of the U.S. Electric Center," which warned that, "[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication."⁷ And just last year, in the Department of Energy's Quadrennial Energy Review, that agency found that the "cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures" and recommended that "system planning must evolve to meet the need for rapid response to system disturbances."⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric-system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber-infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.
2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

⁶ Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Repmt_05.21.13_I.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

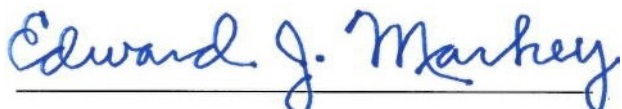
⁸ Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/B4/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

⁹ 83 FR 17913

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?
4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.
5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.
6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?
7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

nitcdtarescnatc

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS
FOREIGN RELATIONS
RANKING MEMBER:
SOUTH PACIFIC, THE PACIFIC,
AND INDIAN NATIONAL CYBERSECURITY POLICY
COMMERCE, ENERGY, AND TRANSPORTATION
RANKING MEMBER:
SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS
SMALL BUSINESS AND ENTREPRENEURSHIP
CHAIRMAN:
U.S. SENATE COMMERCE AND COMPETITIVENESS TASK FORCE

August 13, 2018

Mark A. Gabriel, Administrator and CEO
Western Area Power Administration
PO Box 281213
Lakewood, CO 80228

Dear Mr. Gabriel,

According to recent press reports, state-sponsored groups in Russia were behind a cyberattack on U.S. electric utilities last year.¹ In light of these concerning reports, I write to better understand how you are working to maximize the security of our electric grid and minimize its vulnerabilities to attack.

On July 23, the Wall Street Journal reported that, in 2016 and 2017, hackers backed by the Russian government successfully penetrated the U.S. electric grid through hundreds of power companies and third-party vendors with whom they do business.² Utilizing techniques to access purportedly secure networks, these Russian hackers managed to invade the networks of key utility vendors - companies "who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order."³ Through these vendors, the Russian hackers gained access to the control rooms of U.S. electric utilities, putting them in position to severely disrupt the U.S. power flow. There is now also concern that Russia may be seeking to automate these types of attacks, which could lead to more pervasive and broader hacking and harm to the electric grid.⁴

This recent attack should come as no surprise. In 2013, the Department of Homeland Security (DHS) considered the threat of cyberattack so serious that it issued an alert warning industry and government officials about it.⁵ That same year, I released a report entitled "Electric Grid

¹ Rebecca Smith, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, Wall Street Journal (July 23, 2018), <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ Ellen Nakashima, U.S. warns industry of heightened risk of cyberattack, Washington Post (May 9, 2013), https://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html

Vulnerability: Industry Responses Reveal Security Gaps," which found that the electric grid was the target of ongoing cyberattacks.⁶ In August 2016, the Idaho National Laboratory issued a report entitled "Cyber Threat and Vulnerability Analysis of the U.S. Electric Center," which warned that, "[w]ith utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyberattacks on the North American electric grid continue to grow in frequency and sophistication."⁷ And just last year, in the Department of Energy's Quadrennial Energy Review, that agency found that the "cybersecurity landscape is characterized by rapidly evolving threats and vulnerability, juxtaposed against the slower-moving deployment of defense measures" and recommended that "system planning must evolve to meet the need for rapid response to system disturbances."⁸

Following the release of my 2013 report, the Federal Energy Regulatory Commission (FERC) initiated a series of rulemakings to help address the security of our electric system infrastructure. The most recent of these rules, issued in April 2018, institutes mandatory security controls for transient electronic devices, such as thumb drives, in an attempt to address classic cyber infiltration methods through third party devices.⁹ However, as this most recent incident demonstrates, these security measures do not impede the sophisticated actions now being employed by foreign hackers.

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

- 1, According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.
2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

⁶ Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, prepared by the staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA) (May 21, 2013), https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

⁷ Mission Support Center Analysis Report, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Laboratory (August 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

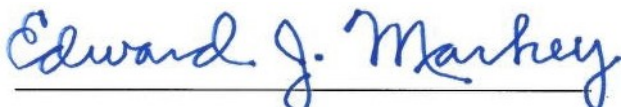
⁸ Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the QER, U.S. Department of Energy (January 2017), <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>

⁹ 83 FR 17913

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?
4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.
5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.
6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?
7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

Thank you in advance for your attention to these requests. If you have any questions about them, please contact Lindsey Griffith of my staff at 202-224-2742.

Sincerely,

A handwritten signature in blue ink that reads "Edward J. Markey". The signature is written in a cursive style and is positioned above a horizontal line.

Edward J. Markey

United States Senator

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.

(b) (5)



2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

a. (b) (5)

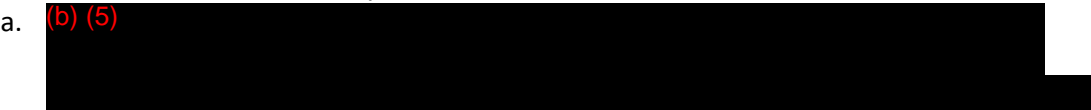


b. (b) (5)



3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?

a. (b) (5)



(b) (5)

b. (b) (5)

c. (b) (5)

d. (b) (5)

e. (b) (5)

f. (b) (5)

4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.

a. (b) (5)

5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.

a. (b) (5)

b. (b) (5)

6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection

Standards — Version 5 — adequately protects against all known cybersecurity vulnerabilities?
Why or why not?

a. (b) (5) [Redacted]

7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

a. (b) (5) [Redacted]

b. (b) (5) [Redacted]

c. (b) (5) [Redacted]

#	Milestones	Date	Status
1	FIN service catalog completed	4/13/2018	Complete
2	FIN connected endpoint inventory	7/27/2018	Complete
3	Endpoint device security profiles, with compliance impact, completed	8/15/2018	In Progress
4	FIN user community structure documented	4/24/2018	Complete
5	Organizational Change Management plan completed	5/24/2018	Complete
6	TTC / TTO / Service Provider mgmt./ownership impact analysis plan developed	9/13/2018	In Progress
7	Managed security services delivery plan	11/30/2018	In Progress
8	Equipment assessment criteria documented	12/28/2018	In Progress
9	User impact analyzed and documented	2/15/2019	In Progress
10	End device migration activities and schedule requirements documented	3/15/2019	In Progress
11	Documentation requirements identified	3/29/2019	In Progress
12	Submit a formal Transmission project proposal via the AMPD process to reconfigure the Field Network and secure it by migrating to TNMS.	4/15/2019	In Progress

To better understand the efforts of electric utilities to protect grid assets from cyberattack, I respectfully ask that you respond to the following questions no later than September 7, 2018:

- 1. According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.

(b) (5)



- 2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

- a. (b) (5)
 - b. (b) (5)
- 

- 3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?

- a. (b) (5)
 - b. (b) (5)
 - c. (b) (5)
- 

- d. (b) (5)
- e. (b) (5)
- f. (b) (5)

4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.

- a. (b) (5)

5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.

- (b) (5)

6. Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards — Version 5 — adequately protects against all known cybersecurity vulnerabilities? Why or why not?

- a. (b) (5)

7. Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?

- (b) (5)

(b) (5)

[Redacted text block]

[Redacted text block]

[Redacted text block]

From: [Jungling, Darren L \(BPA\) - JBB-B1](#)
To: [Dodd Jr, Gary A \(BPA\) - JB-B1](#)
Subject: FW: Signed - Markey letter re Cyber Attacks.pdf
Date: Friday, February 28, 2020 12:58:45 PM
Attachments: [Signed - Markey letter re Cyber Attacks.pdf](#)

Thank-you,
Darren

[Darren L. Jungling](#)
[Supv., Assessment, Awareness, Reporting and Remediation](#)
[Bonneville Power Administration](#)
[U.S. Department of Energy](#)
[503.230.3553 \(v\)](#)
[503.872.7708 \(f\)](#)
[HQ - B193](#)

From: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>
Sent: Monday, September 17, 2018 3:39 PM
To: Barry, Sean P (BPA) - JBB-B1 <spbarry@bpa.gov>; Bauras, Victoria L (BPA) - JBB-B1 <vlbauras@bpa.gov>; Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>; Collier, Alicia N (BPA) - JBB-B1 <ancollier@bpa.gov>; Gilden, Madison M (CONTR) - JB-B1 <mmgilden@bpa.gov>; Jungling, Darren L (BPA) - JBB-B1 <dljungling@bpa.gov>; Kazlas, David A (CONTR) - JBC-B1 <dakazlas@bpa.gov>; Lowe, Richard T (CONTR) - JBB-B1 <rtlowe@bpa.gov>; Mariotti-Jones, Rossella (BPA) - JBC-B1 <rnmarriott@bpa.gov>; Markovitz, Sue (BPA) - JBC-B1 <slmarkovitz@bpa.gov>; McCarrig, Michael T (CONTR) - JBB-B1 <mtmccarrig@bpa.gov>; McGuire, Andrew S (BPA) - JBB-B1 <asmcguire@bpa.gov>; Monk, Rumel D (CONTR) - JBB-B1 <rdmonk@bpa.gov>; Nichols, Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>; Palmer, Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>; Paradis, Ryan C (BPA) - JBC-B1 <rcparadis@bpa.gov>; Quinata, Matthew Y (CONTR) - JBB-B1 <myquinata@bpa.gov>; Rackley, Jessica L (BPA) - JBC-B1 <jlrackley@bpa.gov>; Vink, Amber M (BPA) - JBC-B1 <amvink@bpa.gov>; Wright, Todd R (CONTR) - JBB-B1 <trwright@bpa.gov>
Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

FYSA

From: Marker, Douglas R (BPA) - DIR-7
Sent: Monday, September 17, 2018 3:07 PM
To: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>
Subject: Signed - Markey letter re Cyber Attacks.pdf

Gary – it was a complicated process to complete this with Elliot’s signature but here it is. Thanks for your help.



Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

EXECUTIVE OFFICE

September 11, 2018

The Honorable Edward J. Markey
United States Senate
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter requesting information about the Bonneville Power Administration's (BPA) practices and experience managing the risk of cyber attacks on its transmission system and related facilities. BPA is a Federal power marketing administration responsible for the operation of 15,000 circuit miles of high voltage transmission in the Pacific Northwest. BPA maintains robust monitoring for cyber security and the reliability of its electric systems.

Threats against the electric grid from a cyber perspective are constantly evolving. BPA incorporates lessons learned from the Department of Energy (DOE), the Department of Homeland Security (DHS), and industry best practices; participates in DOE cyber risk identification and mitigation programs, including the federal version of the Cybersecurity Risk Information Sharing Program (CRISP), the Cooperative Protection Program (CPP); and implements the requirements of the DOE Risk Management Framework among other Federal guidance. BPA operates a 24/7 cyber security operations and analysis center.

BPA is subject to mandatory reliability standards of the North American Electric Reliability Corporation (NERC) which are approved by the Federal Energy Regulatory Commission (FERC), including cyber security standards. BPA maintains a close working relationship with DOE Office of Intelligence and Counterintelligence and participates in the joint government-industry Electricity Subsector Coordinating Council (ESCC), the Cyber Mutual Assistance Program, as well as other industry groups with a focus on anticipating and mitigating cyber security risks.

BPA's responses to your questions follow:

1. *According to the Department of Homeland Security, the most recent Russian cyberattacks affected hundreds of companies. Was your company a victim of this most recent attack? If so, please describe how your system was infiltrated and identify the steps you are taking to prevent a future incursion of the same nature.*

BPA was not a victim of this attack.

2. New cyber-vulnerabilities that could pose risks for the grid continue to emerge. These include, but are not limited to, active hacking measures and corruption of third-party firmware or software. Please describe the steps, if any, you are taking to address these types of vulnerabilities.

BPA fully complies with NERC's mandatory reliability standards. BPA maintains a robust security authorization program for acquisition of information technology that is tailored for operational technology. BPA performs offensive research on automated grid technology and penetration testing. BPA operates a 24/7 cyber security operations and analysis center. BPA uses these practices to identify vulnerabilities and to mitigate them.

3. Do you currently utilize security protocols, special measures, or other practices to assess whether current or prospective third-party vendors could pose a cybersecurity threat? If so, please describe them. If not, why not?

BPA ensures that contracts for information and operation technology require application of the Federal Information Security Modernization Act (FISMA). BPA monitors the ownership of its vendors and consults regularly with expert Federal agencies to advise it on the use of vendors.

4. For each of the past five years, how many notices did you receive from the North American Electric Reliability Corporation (NERC) relating to cyber security and containing Recommendations and Essential Actions? For each such notice, please indicate (a) the type of notice, (b) the degree to which the notice related to cybersecurity measures, (c) how many actions were included, and (d) how many of the recommended actions you fully implemented. If you have not implemented any of the actions because they are inapplicable, please also indicate this in your response.

Since 2013, NERC has issued 11 cyber security related Alerts (eight Level 1 Advisories and three Level 2 Recommendations). Several were primarily informational and required no action. BPA responded fully and appropriately to the rest of the alerts.

5. For each of the past five years, have you been subject to an attempted or successful physical or cyberattack? For each year, please indicate (a) the number of attempted and successful physical attacks, (b) the number of attempted and successful cyberattacks, (c) whether any attack caused damage (and if so, please describe the nature of both the attack and the damage caused), (d) the number of attacks reported to FERC, NERC, DHS, DOE, or another authority (and identify which authority in each case), and (e) measures taken to prevent future similar attacks.

BPA is required by NERC Critical Infrastructure Protection Reliability Standards to report cyber incidents that impact the Bulk Electric System (BES) and BES Cyber Systems to the Electricity Information Sharing and Analysis Center (E-ISAC). There have been no reportable incidents in the last five years.

6. *Do you believe that the most recent version of the FERC Critical Infrastructure Protection Standards - Version 5 - adequately protects against all known cybersecurity vulnerabilities? Why or why not?*

Critical Infrastructure Protection (CIP) standards development is an ongoing, iterative process. The process is risk-based and adaptive. They are continually reviewed and updated as threats are identified.

7. *Have you identified any additional vulnerabilities, including as part of an audit of third-party vendors? How do you plan to address any of these additional vulnerabilities?*

BPA identifies vulnerabilities through various means, including vulnerability management, continuous diagnostics, and monitoring and security authorization. BPA addresses potential vulnerabilities appropriately.

I appreciate the opportunity to respond to your questions. If you have additional questions or need further information, please contact me or Sonya Baskerville, BPA's Manager for National Relations, at 202-586-5640.

Sincerely,



Elliot E. Mainzer
Administrator and Chief Executive Officer

From: [Mariotti-Jones,Rossella \(BPA\) - JBC-B1](#)
To: [Nichols,Jon R \(BPA\) - JBC-B1](#)
Subject: RE: Signed - Markey letter re Cyber Attacks.pdf
Date: Thursday, September 20, 2018 11:03:06 AM

(b) (5)

[Redacted]

Regards,

~ ~ ~

Rossella Mariotti-Jones, CISSP

Office of Cyber Security – JBC | Bonneville Power Administration | U.S. Department Of Energy

From: Nichols,Jon R (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:58 AM
To: Mariotti-Jones,Rossella (BPA) - JBC-B1 <rnmarriotti@bpa.gov>
Subject: RE: Signed - Markey letter re Cyber Attacks.pdf

(b) (5)

[Redacted]

Jon Nichols

Cyber Risk Specialist

Office of Cyber Security

Bonneville Power Administration

Desk: (503) 230-4766 | Cell: (b) (6)

From: Mariotti-Jones,Rossella (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:51 AM
To: Nichols,Jon R (BPA) - JBC-B1
Subject: RE: Signed - Markey letter re Cyber Attacks.pdf

I have not heard anything about this since the time Amber forwarded Markey’s request to us. Then suddenly the letter is signed by Elliot and went out. I’m guessing Darren’s group probably had something to do with coming up with the answers, or Gary.

Regards,

~ ~ ~

Rossella Mariotti-Jones, CISSP

Office of Cyber Security – JBC | Bonneville Power Administration | U.S. Department Of Energy

From: Nichols,Jon R (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:43 AM

To: Mariotti-Jones,Rossella (BPA) - JBC-B1 <rnMariotti@bpa.gov>; Markovitz,Sue (BPA) - JBC-B1 <slmarkovitz@bpa.gov>; Nichols,Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>; Palmer,Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>; Paradis,Ryan C (BPA) - JBC-B1 <rcparadis@bpa.gov>; Rackley,Jessica L (BPA) - JBC-B1 <jlrackley@bpa.gov>; Vink,Amber M (BPA) - JBC-B1 <amvink@bpa.gov>

Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

(b) (5)

In anticipation of being asked for input, we developed some preliminary responses located on the share under (b) (2)

Jon Nichols

Cyber Risk Specialist

Office of Cyber Security

Bonneville Power Administration

Desk: (503) 230-4766 | Cell: (b) (6)

From: Dodd Jr,Gary A (BPA) - JB-B1

Sent: Monday, September 17, 2018 3:39 PM

To: Barry,Sean P (BPA) - JBB-B1; Bauras,Victoria L (BPA) - JBB-B1; Callaway III,George M (BPA) - JBB-B1; Collier,Alicia N (BPA) - JBB-B1; Gilden,Madison M (CONTR) - JB-B1; Jungling,Darren L (BPA) - JBB-B1; Kazlas,David A (CONTR) - JBC-B1; Lowe,Richard T (CONTR) - JBB-B1; Mariotti-Jones,Rossella (BPA) - JBC-B1; Markovitz,Sue (BPA) - JBC-B1; McCarrig,Michael T (CONTR) - JBB-B1; McGuire,Andrew S (BPA) - JBB-B1; Monk,Rumel D (CONTR) - JBB-B1; Nichols,Jon R (BPA) - JBC-B1; Palmer,Scott M (BPA) - JBC-B1; Paradis,Ryan C (BPA) - JBC-B1; Quinata,Matthew Y (CONTR) - JBB-B1; Rackley,Jessica L (BPA) - JBC-B1; Vink,Amber M (BPA) - JBC-B1; Wright,Todd R (CONTR) - JBB-B1

Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

FYSA

From: Marker,Douglas R (BPA) - DIR-7

Sent: Monday, September 17, 2018 3:07 PM

To: Dodd Jr,Gary A (BPA) - JB-B1 <gadodd@bpa.gov>

Subject: Signed - Markey letter re Cyber Attacks.pdf

Gary – it was a complicated process to complete this with Elliot’s signature but here it is. Thanks for your help.

From: [Rackley, Jessica L \(BPA\) - JBC-B1](#)
To: [Vink, Amber M \(BPA\) - JBC-B1](#)
Subject: FW: Signed - Markey letter re Cyber Attacks.pdf
Date: Friday, September 21, 2018 10:27:12 AM
Attachments: [Signed - Markey letter re Cyber Attacks.pdf](#)

Goodness.

Jessica Rackley

Office of Cyber Security
Bonneville Power Administration
U.S. Department of Energy

From: Nichols, Jon R (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:43 AM
To: Mariotti-Jones, Rossella (BPA) - JBC-B1; Markovitz, Sue (BPA) - JBC-B1; Nichols, Jon R (BPA) - JBC-B1; Palmer, Scott M (BPA) - JBC-B1; Paradis, Ryan C (BPA) - JBC-B1; Rackley, Jessica L (BPA) - JBC-B1; Vink, Amber M (BPA) - JBC-B1
Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

(b) (5)

In anticipation of being asked for input, we developed some preliminary responses located on the share under (b) (2)

Jon Nichols

Cyber Risk Specialist
Office of Cyber Security
Bonneville Power Administration
Desk: (503) 230-4766 | Cell: (b) (6)

From: Dodd Jr, Gary A (BPA) - JB-B1
Sent: Monday, September 17, 2018 3:39 PM
To: Barry, Sean P (BPA) - JBB-B1; Bauras, Victoria L (BPA) - JBB-B1; Callaway III, George M (BPA) - JBB-B1; Collier, Alicia N (BPA) - JBB-B1; Gilden, Madison M (CONTR) - JB-B1; Jungling, Darren L (BPA) - JBB-B1; Kazlas, David A (CONTR) - JBC-B1; Lowe, Richard T (CONTR) - JBB-B1; Mariotti-Jones, Rossella (BPA) - JBC-B1; Markovitz, Sue (BPA) - JBC-B1; McCarrig, Michael T (CONTR) - JBB-B1; McGuire, Andrew S (BPA) - JBB-B1; Monk, Rumel D (CONTR) - JBB-B1; Nichols, Jon R (BPA) - JBC-B1; Palmer, Scott M (BPA) - JBC-B1; Paradis, Ryan C (BPA) - JBC-B1; Quinata, Matthew Y (CONTR) - JBB-B1; Rackley, Jessica L (BPA) - JBC-B1; Vink, Amber M (BPA) - JBC-B1; Wright, Todd R (CONTR) - JBB-B1
Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

FYSA

From: Marker, Douglas R (BPA) - DIR-7
Sent: Monday, September 17, 2018 3:07 PM

To: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>

Subject: Signed - Markey letter re Cyber Attacks.pdf

Gary – it was a complicated process to complete this with Elliot’s signature but here it is. Thanks for your help.

From: [Mariotti-Jones,Rossella \(BPA\) - JBC-B1](#)
To: [Nichols,Jon R \(BPA\) - JBC-B1](#)
Subject: RE: Signed - Markey letter re Cyber Attacks.pdf
Date: Wednesday, October 3, 2018 7:21:57 AM

Did you get anything else back from Amber in writing or in person about this?
We could bring it up at one of our meetings.

Regards,

~ ~ ~

Rossella Mariotti-Jones, CISSP
Office of Cyber Security – JBC | Bonneville Power Administration | U.S. Department Of Energy

From: Nichols,Jon R (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:58 AM
To: Mariotti-Jones,Rossella (BPA) - JBC-B1 <rmariotti@bpa.gov>
Subject: RE: Signed - Markey letter re Cyber Attacks.pdf

(b) (5)
[Redacted]

Jon Nichols

Cyber Risk Specialist
Office of Cyber Security
Bonneville Power Administration
Desk: (503) 230-4766 | Cell: (b) (6)

From: Mariotti-Jones,Rossella (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:51 AM
To: Nichols,Jon R (BPA) - JBC-B1
Subject: RE: Signed - Markey letter re Cyber Attacks.pdf

I have not heard anything about this since the time Amber forwarded Markey’s request to us. Then suddenly the letter is signed by Elliot and went out. I’m guessing Darren’s group probably had something to do with coming up with the answers, or Gary.

Regards,

~ ~ ~

Rossella Mariotti-Jones, CISSP
Office of Cyber Security – JBC | Bonneville Power Administration | U.S. Department Of Energy

From: Nichols,Jon R (BPA) - JBC-B1
Sent: Thursday, September 20, 2018 10:43 AM
To: Mariotti-Jones,Rossella (BPA) - JBC-B1 <rmariotti@bpa.gov>; Markovitz,Sue (BPA) - JBC-B1 <slmarkovitz@bpa.gov>; Nichols,Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>; Palmer,Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>; Paradis,Ryan C (BPA) - JBC-B1 <rcparadis@bpa.gov>; Rackley,Jessica L

(BPA) - JBC-B1 <jlrackley@bpa.gov>; Vink,Amber M (BPA) - JBC-B1 <amvink@bpa.gov>

Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

(b) (5)

In anticipation of being asked for input, we developed some preliminary responses located on the share under (b) (2)

Jon Nichols

Cyber Risk Specialist

Office of Cyber Security

Bonneville Power Administration

Desk: (503) 230-4766 | Cell: (b) (6)

From: Dodd Jr, Gary A (BPA) - JB-B1

Sent: Monday, September 17, 2018 3:39 PM

To: Barry, Sean P (BPA) - JBB-B1; Bauras, Victoria L (BPA) - JBB-B1; Callaway III, George M (BPA) - JBB-B1; Collier, Alicia N (BPA) - JBB-B1; Gilden, Madison M (CONTR) - JB-B1; Jungling, Darren L (BPA) - JBB-B1; Kazlas, David A (CONTR) - JBC-B1; Lowe, Richard T (CONTR) - JBB-B1; Mariotti-Jones, Rossella (BPA) - JBC-B1; Markovitz, Sue (BPA) - JBC-B1; McCarrig, Michael T (CONTR) - JBB-B1; McGuire, Andrew S (BPA) - JBB-B1; Monk, Rumel D (CONTR) - JBB-B1; Nichols, Jon R (BPA) - JBC-B1; Palmer, Scott M (BPA) - JBC-B1; Paradis, Ryan C (BPA) - JBC-B1; Quinata, Matthew Y (CONTR) - JBB-B1; Rackley, Jessica L (BPA) - JBC-B1; Vink, Amber M (BPA) - JBC-B1; Wright, Todd R (CONTR) - JBB-B1

Subject: FW: Signed - Markey letter re Cyber Attacks.pdf

FYSA

From: Marker, Douglas R (BPA) - DIR-7

Sent: Monday, September 17, 2018 3:07 PM

To: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>

Subject: Signed - Markey letter re Cyber Attacks.pdf

Gary – it was a complicated process to complete this with Elliot’s signature but here it is. Thanks for your help.

Weakness ID	Weakness Control	Weakness Risk	Weakness Details from SAR	Weakness Corrective Action Recommendation	POA&M ID	ISO	Corrective Action Plan Details (Milestones and Dates)	Scheduled Completion Date	Resources - Funding Required	Resources - FTE Time Estimate	SME	Status	POA&M Running History	Evidence
EA21-2017-TS-01	RA-3	Finding 1	BPA has not established documented or fully implemented a formal RMA or RMF for BPA IT resources. [DOE Order 205.1B 3.a.(5) 4.b. 5.b.(3); NIST SP 800-37 Revision 1 2.1; NIST SP 800-53 Revision 4 RA-3]		EA21-2017-TS-01		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-02	CA-1 CA-6 PM-10	Finding 2	Transmission Services is operating the TNMS without an ATO ATC or a risk determination letter. [DOE Order 205.1B Change 3; NIST SP 800-53 Revision 4 CA-1 CA-6 PM-10]		EA21-2017-TS-02		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-03	RA-3	Deficiency 1	Transmission Services has not conducted a risk assessment to identify specific risk and how any risk impacts Transmission Services resources. [DOE Order 205.1B Change 3 4.b.(2); NIST SP 800-53 Revision 4 RA-3]		EA21-2017-TS-03		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-04	AU-6	Deficiency 2	Transmission Services does not review and analyze information system audit records on the classified FMS at least weekly for indications of inappropriate or unusual activity and does not report findings to designated organizational officials. [DOE Order 205.1B Change 3; CNSSI 1253-AU-6; FMS SSP Paragraph 5.4.f.]		EA21-2017-TS-04		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-05	SI-3	Deficiency 3	Transmission Services does not perform periodic scans of the FMS at least weekly or real-time scans of files from external sources as the files are downloaded opened or executed in accordance with organizational security policy and does not quarantine malicious code or send an alert to the system administrator in response to malicious code detection. [DOE Order 205.1B Change 3; CNSSI 1253-SI-3]	Transmission Services has implemented several strong configuration management processes including establishing baseline configurations for the operating systems and network devices and applying formal configuration management processes requiring cyber security review and approval. However the lack of periodic validation of security controls and the lack of applying the same processes and procedures across all systems to include the classified system detracts from the overall effectiveness of the configuration management process.	EA21-2017-TS-05		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-06	AC-20	Deficiency 4	Transmission Services has not established terms and conditions consistent with any trust relationships regarding the IC laptops that are connected by maintenance personnel to the FIN which results in increased risk to FIN because these laptops can introduce malware onto the FIN. [DOE Order 205.1B Change 3; NIST SP 800-53 Revision 4 AC-20].		EA21-2017-TS-06		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-07		OFI 1	Transmission Services should consider clearly documenting how all controls inherited from BPA Headquarters that apply to Transmission Services systems such as training authorization processes and planning are implemented. Transmission Services should also consider clearly documenting how it implements controls applied directly by Transmission Services.		EA21-2017-TS-07		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-08		OFI 2	Transmission Services should consider completing a comprehensive inventory of all the assets that are under its operational control.		EA21-2017-TS-08		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-09		OFI 4	Transmission Services should consider performing self-assessments on all systems at least annually. The self-assessments should test all NIST SP 800-53 or CNSSI 1253 security controls commensurate with the security categorization for the system being assessed.		EA21-2017-TS-09		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-10		OFI 5	Transmission Services should consider completing BIAs for all of its networks.		EA21-2017-TS-10		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-11		OFI 6	Transmission Services should consider requiring some form of patch and vulnerability management checking for the non-NERC CIP devices e.g. non-FIN administered laptops that connect on an ad hoc basis to the FIN to preclude the introduction of malicious software onto its networks.		EA21-2017-TS-11		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-12		OFI 7	Transmission Services should consider establishing and documenting a formal vulnerability management process that includes specific timeframes for the remediation of vulnerabilities identified through the vulnerability scanning process as indicated in the BITA.		EA21-2017-TS-12		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-13		OFI 8	Transmission Services should consider putting into place a process to perform regular patching of the FMS operating system and antivirus.		EA21-2017-TS-13		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-14		OFI 9	Transmission Services should consider performing a more aggressive sweep of PSPs for the use of unauthorized wireless devices especially the use of cellular phones as personal hotspots to prevent the unauthorized bridging of isolated networks to the internet.		EA21-2017-TS-14		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-15		OFI 10	Transmission Services should consider conducting regular discovery scans of its networks to verify that IPMI interfaces do not have default credentials enabled and to ensure IPMI interfaces cannot be used for access to servers from the network.		EA21-2017-TS-15		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-16		OFI 11	Transmission Services should consider ensuring that all default account passwords are changed before network equipment or systems are placed into production and enabling configurations that limit access to administrative interfaces.		EA21-2017-TS-16		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-17		OFI 12	Transmission Services should consider employing internal network-based IDSs and ensuring that there is an ability to detect malicious traffic traversing the internal network.		EA21-2017-TS-17		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-18		OFI 13	Transmission Services should consider ensuring that Splunk logs are collecting and recording all data necessary to support incident identification and response (e.g. source IP addresses).		EA21-2017-TS-18		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
EA21-2017-TS-19		OFI 14	Transmission Services should consider ensuring that attribution can be directly assigned to all personnel who have access to servers and verify that the ability to add USB devices to servers is blocked according to site policy. Additionally Transmission Services should consider ensuring that an alert is generated any time a USB device is connected to a NSI computer where USB connections are not authorized.		EA21-2017-TS-19		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							

EA21-2017-TS-20		OFI 15	Transmission Services should consider designing and implementing an intrusion detection plan for the FIN.		EA21-2017-TS-20		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement						
EA21-2017-TS-21		OFI 16	Transmission Services should consider ensuring that updates are performed on outdated software and that unused software applications are removed from systems on a regularly scheduled basis that is defined in a documented process and procedure.		EA21-2017-TS-21		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement						
EA21-2017-TS-22		OFI 17	Transmission Services should consider developing consistent processes and procedures for software patching across all its systems to eliminate vulnerabilities from the network devices and systems.		EA21-2017-TS-22		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement						

Weakness ID	Weakness Control	Weakness Risk	Weakness Data Is from SAR	Weakness Corrective Action Recommendation	POA&M ID	ISO	Corrective Action Plan Details (Milestones and Dates)	Scheduled Completion Date	Resources - Funding Required	Resources - FTE Time Estimate	SME	Status	POA&M Running History	Evidence
FLD-FIN-121416-1	CA-7 CM-8 IA-3 SA-4 SC-17 SI-4 PM-5	Level	There is no properly managed hardware inventory of authorized devices in the environment.	(b) (5)	FLD-FIN-121416-1		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-2	CA-7 CM-2 CM-8 CM-10 CM-11 SA-4 SC-18 SC-34 SI-4 PM-5	Level	There is no properly managed software inventory of authorized applications in the environment.		FLD-FIN-121416-2		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-3	CA-7 CM-2 CM-3 CM-5 CM-6 CM-7 CM-8 CM-9 CM-11 MA-4 RA-5 SA-4 SC-14 SC-34 SI-2 SI-4	Level	There are no configuration baselines for hardware and software applications within the environment.		FLD-FIN-121416-3		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-4	CA-2 CA-7 RA-5 SC-34 SI-4 SI-7	Level	There is no continuous vulnerability scanning or patch management.		FLD-FIN-121416-4		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-5	CA-7 SC-39 SC-44 SI-3 SI-4 SI-8	Level	There is no managed anti-virus or anti-malware program.		FLD-FIN-121416-5		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-6	CP-9 CP-10 MP-4	Level	There is no managed business continuity and disaster recovery program.		FLD-FIN-121416-6		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-7	AC-4 CA-3 CA-7 CA-9 CM-2 CM-3 CM-5 CM-6 CM-8 MA-4 SC-24 SI-4	Level	There is no managed change and configuration management program.		FLD-FIN-121416-7		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-8	AC-4 CA-7 CA-9 CM-2 CM-6 CM-8 SC-20 SC-21 SC-22 SC-41 SI-4	Level	There is no managed list of approved and unapproved ports protocols and services.		FLD-FIN-121416-8		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-9	AC-2 AC-6 AC-17 AC-19 CA-7 IA-2 IA-4 IA-5 SI-4	Level	There is no managed list of approved administrative user and shared accounts.		FLD-FIN-121416-9		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-10	AC-4 AC-17 AC-20 CA-3 CA-7 CA-9 CM-2 SA-9 SC-7 SC-8 SI-4	Level	There is no visibility monitoring or management of the interconnections between networks.		FLD-FIN-121416-10		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-11	AC-23 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-8 AU-9 AU-10 AU-11 AU-12 AU-13 AU-14 CA-7 IA-10 SI-4	Level	There is no managed continuous monitoring program.		FLD-FIN-121416-11		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-12	AC-2 AC-3 AC-7 AC-11 AC-12 CA-7 IA-5 IA-10 SC-17 SC-23 SI-4	Level	There is no managed account monitoring program.		FLD-FIN-121416-12		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-13	AC-8	Level	There are no warning banners.		FLD-FIN-121416-13		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-14	CM-9 AC-5 AC-3 AC-6 PE-5 PE-4	Level	There is no separation of duties.		FLD-FIN-121416-14		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-15	IR-1 IR-2 IR-3 IR-4 IR-5 IR-6 IR-7 IR-8 IR-10	Level	There is no managed incident response program.		FLD-FIN-121416-15		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-FIN-121416-16	AC-4 CA-3 CA-9 SA-8 SC-20 SC-21 SC-22 SC-32 SC-37 PL-2	Level	There is no managed security engineering program.		FLD-FIN-121416-16		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							

Weakness ID	Weakness Control	Weakness Risk	Weakness Details from SAR	Weakness Corrective Action Recommendation	POA&M ID	ISO	Corrective Action Plan Details (Milestones and Dates)	Scheduled Completion Date	Resources - Funding Required	Resources - FTE Time Estimate	SME	Status	POA&M Running History	Evidence
FLD-RedTeam-102014-1		High	Malicious activity using Powershell and PSEXec was not detected on workstations.	(b) (5)	FLD-RedTeam-102014-1		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-RedTeam-102014-2		High	Malicious activity using Powershell and PSEXec was not detected on workstations.		FLD-RedTeam-102014-2		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-RedTeam-102014-3		High	Many service accounts and user accounts (both regular and elevated) were cracked within 24 hours because they only used 8 characters and a known pattern.		FLD-RedTeam-102014-3		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-RedTeam-102014-4		High	Default passwords were used on serveral network devices and appliances.		FLD-RedTeam-102014-4		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-RedTeam-102014-5		High	The Microsoft workstation firewall is able to be modified and not block the opening of local ports. The firewall modification activity was not detected.		FLD-RedTeam-102014-5		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-RedTeam-102014-6		High	Systems failed to detect known malware such as Veil, Invoke-Mimikatz and F-pipe.		FLD-RedTeam-102014-6		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							
FLD-RedTeam-102014-7		High	Information was collected on instrument controllers on the FIN network and exfiltrated outside the FIN.		FLD-RedTeam-102014-7		Milestone 1 [12/31/2018] - Develop Action Plans or Provide Position Statement							

From: [Collier, Alicia N \(BPA\) - JBB-B1](#)
To: [DiGenova, Jeffrey A \(BPA\) - TT-DITT-2](#); [Ngo, Huy N \(BPA\) - TT-DITT-2](#); [Raschio, Peter J \(BPA\) - TTS-DITT-2](#); [Jones, Rustin P \(CONTR\) - TT-MODD](#); [Krigbaum, Forrest M \(BPA\) - TT-MODD](#); [Banker, William P \(CONTR\) - TT-MODD](#); [Robinson, Brian S \(CONTR\) - TT-B-MODD](#); [Gallman Jr, Stephen W \(BPA\) - TTOM-DITT-1](#)
Cc: [ADL, JBC ALL](#); [Jungling, Darren L \(BPA\) - JBB-B1](#); [Callaway III, George M \(BPA\) - JBB-B1](#); [Bauras, Victoria L \(CONTR\) - JBB-B1](#); [Comingo, Amanda M \(CONTR\) - JBB-B1](#); [Quinata, Matthew Y \(CONTR\) - JBB-B1](#); bjmurray@bpa.gov; smpalmer@bpa.gov; rnmariotti@bpa.gov; rcparadis@bpa.gov; slweidkamp@bpa.gov; jlrackley@bpa.gov; amvink@bpa.gov; jrnichols@bpa.gov
Subject: STATUS: CCN Red Team (TO) POAM Remediation Status for the Week Ending November 10, 2017
Date: Thursday, November 9, 2017 11:18:25 AM

All,

This will be the LAST weekly status update for this remediation. I will work with ISO, ISSO and SMES on the TSI-OVCI DTS Remediation Closure Report and package. I am going to propose that we gather the information on the items with residual risk (memos) and put this one thorough our POA&M Remediation closure process. I will be reaching out to the team in the next week or two as I draft the POA&M Remediation Closure Package.

In Progress:

CCN-RedTeam-102014-5 (Due 9/1/17): Information received from Pete Raschio working compile evidence for projects listed in milestone. Creating Retest CRM.

CCN-RedTeam-102014-9 (Due 6/30/17): CRM2321905 – Failed, Need IO/ISO to provide a risk acceptance statement.

Submitted to Retest:

CCN-RedTeam-102014-8 (Due 6/30/17): CRM2321903 – Retest with assessor. Needs clarification of new evidence. Alicia Collier to circle back with Rustin Jones.

Awaiting CISO Action/Residual Risk:

CCN-RedTeam-102014-4 (Due 9/30/17): A risk acceptance memorandum has been prepared by the ISO with consult and coordination through the information owner (IO). The Remediation Team will work with the CISO for follow-up and presentation to the Authorizing Official.

CCN-RedTeam-102014-7 (Due 6/30/17): A risk acceptance memorandum has been prepared by the ISO with consult and coordination through the information owner (IO). The Remediation Team will work with the CISO for follow-up and presentation to the Authorizing Official.

Complete:

CCN-RedTeam-102014-1: CRM2321892 – Complete - Passed

CCN-RedTeam-102014-2: CRM 2267114 Complete – Mitigated Moderate

CCN-RedTeam-102014-3: CRM 2267182 Complete - Passed

CCN-RedTeam-102014-6: CRM CRM2267191 Complete – Passed

CCN-RedTeam-102014-10: CRM2291167 Complete-Passed

For additional details please see the [CCN Red Team POAM Tracking Worksheet](#).

Let me know if there any questions.

Thank you,

Alicia Collier

Office of Cyber Security

BONNEVILLE POWER ADMINISTRATION

US DEPARTMENT OF ENERGY

bpa.gov | P 503-230-4485

From: [Dodd Jr, Gary A \(BPA\) - JB-B1](#)
To: [Jungling, Darren L \(BPA\) - JBC-B1](#)
Subject: RE: Vulnerability Status RT
Date: Monday, February 24, 2020 10:26:42 AM

I've asked JBC to take a look. (b) (5)

From: Jungling, Darren L (BPA) - JBB-B1
Sent: Monday, February 24, 2020 8:09 AM
To: Nichols, Jon R (BPA) - JBC-B1; Dodd Jr, Gary A (BPA) - JB-B1
Cc: Callaway III, George M (BPA) - JBB-B1; Palmer, Scott M (BPA) - JBC-B1
Subject: RE: Vulnerability Status RT

Thanks Jon!

Thank-you,
Darren

[Darren L. Jungling](#)
[Supv., Assessment, Awareness, Reporting and Remediation](#)
[Bonneville Power Administration](#)
[U.S. Department of Energy](#)
[503.230.3553 \(v\)](#)
[503.872.7708 \(f\)](#)
[HQ - B193](#)

From: Nichols, Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>
Sent: Monday, February 24, 2020 8:00 AM
To: Jungling, Darren L (BPA) - JBB-B1 <dljungling@bpa.gov>; Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>
Cc: Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>; Palmer, Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>
Subject: RE: Vulnerability Status RT

Darren,

I have reviewed Scott's comments and I concur. I have no information to add.

Thanks,

Jon Nichols

Cyber Risk Specialist
Office of Cyber Security
Bonneville Power Administration
Desk: (503) 230-4766 | Cell: (b) (6)

From: Jungling, Darren L (BPA) - JBB-B1 <[dljungling@bpa.gov](mailto:djungling@bpa.gov)>
Sent: Thursday, February 20, 2020 6:31 AM
To: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>
Cc: Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>; Nichols, Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>; Palmer, Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>
Subject: RE: Vulnerability Status RT

Hey Gary,

Jon is out until Monday, 2/24. I have asked Scott to finishing up his comments and provide an update this morning.

Thank-you,
Darren

Darren L. Jungling
Supv., Assessment, Awareness, Reporting and Remediation
Bonneville Power Administration
U.S. Department of Energy
503.230.3553 (v)
503.872.7708 (f)
HQ - B193

From: Jungling, Darren L (BPA) - JBB-B1 <[dljungling@bpa.gov](mailto:djungling@bpa.gov)>
Sent: Tuesday, February 18, 2020 8:25 AM
To: Nichols, Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>; Palmer, Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>
Cc: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>; Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>
Subject: Vulnerability Status RT

Hey Guys,

There is a distinct possibility that the “Red Team” report will be release under a FOIA request. The Front Office has asked Gary to provide a status of where we are now, versus when you conducted the assessment.

Gary has created a folder on the root of JB labeled “RT”. You will find a spreadsheet with the headers of Comment, Status and Verification. Please review the spreadsheet and provide your comments on each of the items. Please add a column to the right of Verification with your name so that we can see which of you has made a particular comment.

(b) (2)

(b) (6)

Scott, if you could make your pass today and then Jon tomorrow, it will provide Gary time to ask any clarifying questions that he might have based on your comments.

Please let Gary, George and me know when you are done.

Thank-you,
Darren

Darren L. Jungling
Supv., Assessment, Awareness, Reporting and Remediation
Bonneville Power Administration
U.S. Department of Energy
503.230.3553 (v)
503.872.7708 (f)
HQ - B193

From: [Dodd Jr, Gary A \(BPA\) - JB-B1](#)
To: [McGuire, Andrew S \(BPA\) - JBB-B1](#)
Subject: FW: 2014 Red Team Vulnerability Notes Spreadsheet
Date: Monday, March 2, 2020 10:18:26 AM
Attachments: [Vulnerability Status Red Team 2014-Scott.xlsx](#)

-----Original Message-----

From: Palmer, Scott M (BPA) - JBC-B1 <smpalmer@bpa.gov>
Sent: Thursday, February 20, 2020 6:46 AM
To: Jungling, Darren L (BPA) - JBB-B1 <dljungling@bpa.gov>; Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>; Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>
Cc: Nichols, Jon R (BPA) - JBC-B1 <jrnichols@bpa.gov>
Subject: 2014 Red Team Vulnerability Notes Spreadsheet

Morning-

Attached to this message are the notes I had for the 2014 Red Team Vulnerability spreadsheet. I created a column with my name on it and conferred with Jon to make sure I didn't miss anything. The last half of the spreadsheet would have been a lot of repetition so it is implied that the comments for the first half's larger questions apply to the last half.

The file is located here:

(b) (2)

The file name with my input is:

(b) (2)

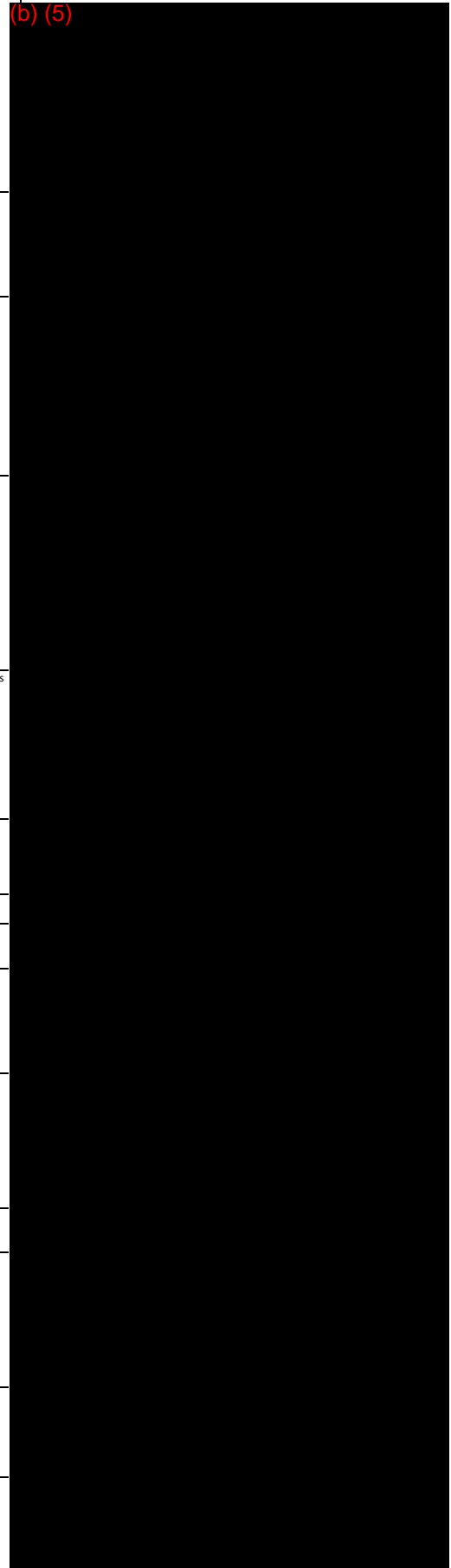
Please let me know if there are any questions or I can help with anything else.

Scott Palmer
Cyber Risk Specialist
Office of Cyber Security
Bonneville Power Administration

Item	Page	Comment	Status	Verification
1	4	During the compromise, the team was able to exfiltrate large amounts of sensitive BPA data without detection.	It is unlikely this could take place today because we monitor for activity.	
2	4	A malicious Excel file was attached to these emails that, when executed, provided a means to bypass network defenses and ability to remotely access the BPA HQ network from the outside.	We have several protections in place including a very robust phishing/phishing training program, Sophos, Einstein and other tools that we did not have then.	
3	4	Employing password guessing techniques over a 28 day period, they identified several commonly used password combinations at BPA.	The Cyber Security Operations and Analysis Center is much more mature now, this could not take place unnoticed. As well, BPA IT's policy requires much larger passwords of 15 characters or more today, AND we have deployed Multifactor Authentication	
4	5	The attackers identified, and were able to take control of, over 30 physical security cameras and numerous appliances connected to the network, mostly due to default configurations.	Cyber regularly looks for these kinds of flaws and IT has brought the PACS system under both FISMA and NERC CIP. This could not be done in the same way if at all today.	
5	5	From inside the BPA HQ network, the team was able to perform lateral movement within and between other internal BPA networks.	The Cyber Security Operations and Analysis Center is much more mature now, this could no longer take place unnoticed.	During the last two EA-60 visits the CSOAC demonstrated its ability to detect lateral movement
6	5	The team was able to access and install malware on 38 workstations that are routinely and almost constantly connect to the FIN (Field Information Network) and the business administrative network.		
7	5	The air-gapping is given pre-eminence to the exclusion of good cyber security practice such as centralized event logging and correlation.		
8	5	In addition, the team successfully infiltrated the Control Center DMZ (a sub network that contains and exposes external-facing services to the Internet).		
9	5	The simulated attackers were able to remotely connect to this network using BPA HQ network credentials.	The use of multifactor authentication would prevent this today.	
10	5	They then were able to guess administrator credentials through password reuse and pattern matching.	Password complexity requirements, checked through automated means were implemented after the attack. Multifactor authentication renders password guessing irrelevant.	
11	5	The attackers were able to modify webpages of DGOZ internal websites, gain full access to an internal file server and deploy malicious code on internal web pages.		
12	5	The exercise has proven that an external threat can successfully penetrate internal BPA systems with minimal detection or response.	The kind of attack that was demonstrated in this exercise would not be successful today and would be detected.	
13	5	Improved training and awareness.	BPA has implemented a very robust and extensive internal phishing program that includes user training, the program continues to raise the bar on difficulty and results show that employees have improved markedly.	

Scott

(b) (5)



14	5	Better communication on incident response.	The CSOAC has regular contact with the Transmission NSOC.	
15	5	Greater visibility for the Cyber Security Operations and Analysis Center from all areas of BPA; Information Technology, Transmission Field, and the Control Center.	The visibility the CSOAC has in all areas has improved. Transmission Technology plan for integration and monitoring of networks is an important step that is in process.	
16	8	They began by manually probing the external servers for well known vulnerabilities using a "low and slow" strategy to avoid detection.		
17	8	They were able to identify several servers in the 170.160.x.x range.		see previous
18	8	Next they probed the identified servers using NMAP, on a limited set of ports, to determine which ones were accessible from outside the BPA network.		see previous
19	8	While these probes required several days to complete, they were not noticed by BPA.		see previous
20	8	External cross-site scripting vulnerabilities were found but not utilized in this attack.		see previous
21	8	Potential SQL-injections were found but the attackers		see previous
22	8	A remote file inclusion vulnerability was found but not weaponized.		see previous
23	8	The scans by DirBuster were inadvertently detected by DoE's Cooperative Protection Plan (CPP) sensors when a User-Agent string was detected by canned IDS signatures. o It took 10 days for BPA's Cyber Security to be notified of this detection, indicating a weakness in BPA's Incident Response process.		see previous
24	8	An FTP server allowing anonymous file uploading and downloading was discovered but was not utilized in this attack		see previous
25	8	Several SMTP mail servers were identified. Three of the mail servers allowed outside users to email internal users while faking the source mailing address as an internal user.		see previous
26	8	On one of the mail servers, Sophos blocks the faked sending address but gives a warning message with a Sophos link to where the spoofed address can be white-listed. This allowed the attackers to bypass the protection mechanism and successfully send malicious email into the organization.	This vulnerability was closed during the exercises.	see previous
27	8	The Team tested the use of an infected MS Excel file on a machine built with Microsoft Forefront. The Microsoft Anit-malware software did not detect the malware.		see previous
28	9	The attackers created an email concerning a news article that appeared to originate from www.bpa.gov.	This vulnerability was closed during the exercises.	see previous
29	10	Team had to determine an easy way to maintain persistence with the code giving them access across logins. The login.bat file was chosen as an executable that could be appended by the malware.	This vulnerability was closed during the exercises.	see previous
30	10	Using the command "c >- net accounts", the Team were able to discover the password policy for BPA. Using this information they discovered the maximum number of logon attempts available before the account locked. Additionally, if an account was inadvertently locked they knew how long before it would unlock automatically.		see previous
31	11	Next, the team attempted four passwords per account every 30-60 minutes for every account.		see previous
32	11	In addition to identifying the accounts the attackers could exploit, they were also able to identify commonly used password combinations.		see previous
33	11	This password guessing scan ran over the entire business administrative network for over a month and was only detected by one group, Critical Business Systems (JC). The account activity was discovered after JC began leveraging the new instance of Splunk. Splunk is software implemented and used by the Cyber Security Operations and Analysis Center (CSOAC).	Splunk and its implementation continues today and is more mature, and continues to mature everyday. As well, with Multifactor authentication renders passwords irrelevant.	see previous
34	11	The Team chose to execute "low-and-slow" NMAP port scans of ports 80 and 443 on the entire 10.0.0.0/8 subnet resulting in approximately 3248 responses. The rationale for the "low-and-slow" scan was to prevent any potential Host-based Intrusion Prevention System (HIPS) detecting the scans.		see previous
35	11	During the scan, approximately 30 physical security cameras were found and accessible through HTTP/HTTPS. Password guessing, along with user manuals for each make and model of camera, allowed the Team to identify default passwords on numerous devices.		see previous

36	11	Other default administrator account/password combinations were found for			see previous
36a	11	• A legacy PBX system			see previous
36b	11	• 3 Quantun Scalar backup systems			see previous
36c	11	• A power meter			see previous
36d	11	• IP-enabled audio codecs			see previous
36e	11	• A barcode device			see previous
36f	11	• A DS3 device			see previous
37	11	Also found was an Integrated Lights-Out-Management (LOM) device with "emergency admin password bypass" enabled.			see previous
38	12	The entire page is about obtaining credentials			see previous
39	14	The attackers used the Microsoft Sysinternals tool "PsExec" to run "Mimkatz" on all workstations used by domain administrators resulting in credentials for all domain administrators. "PsExec" is commonly used by Windows system administrators so the use of it in logs would not raise suspicion. Additionally, it would not be blocked by protection software. "Mimkatz" captures, in clear text, the credentials of any account that was authenticated on the server since last boot.			see previous
40	14	This process secured the NTDS.dit file from the domain controller. Using			see previous
41	14	The attackers assumed an eight character password that started with a capital letter followed by a lowercase letter and all combinations for the remaining six characters (e.g. "Seattle1"). Using this mask the team began trying to crack those hashes to obtain their plain-text passwords. The result, over 10% of the BUD domain fell in four days.			see previous
42	15	Again using the LDAP dumps, the attackers found approximately 113 machines with "SPC ATG 32bit" in the description and whose names ended in "WIN7".			see previous
43	15	A simple ping sweep of the 113 SPC ATG laptops found in the LDAP dumps, the attackers found that about half of the 113 "SPC ATG" laptops are connected to the BUD network at any given time.			see previous
44	17	While the SPC laptops were connected to the BUD domain, the malware was placed on the victim machines through the Microsoft PSEXEC tool using a BUD Desktop Administrator account.			see previous
45	17	The malware captured screenshots of the SPC laptop's desktop every 10 minutes (for any user that logged in), detected if the SPC laptop was on BUD or not, notified the attackers when the laptop was plugged into BUD again, and uploaded the pictures and network information files to the attackers' C&C server on the Internet			see previous
46	17	The attackers were able to guess the BUD password for a user account belonging to a foreman in Montana.	Multifactor authentication renders password guessing irrelevant.		see previous
47	17-18	When the attackers logged into BUD using this account and scoured the foreman's file shares for any file with the word "password" in it, they found a document that contained Level 1 and Level 2 passwords for a D400 device.			see previous
48	18	Documentation also showed that inside the DGOZ, they had changed the Remote Desktop TCP port to 15001, instead of the default 3389.			see previous
49	18	Using a captured BUD user account, the attackers started information mining mapped files shares associated with the user's account.			see previous
50	18	Using the information discovered about the DGOZ, the attackers created a rudimentary port scanner on MyPC (using PowerShell) and found that they were able to connect to remote desktops on many DGOZ machines from BUD.			see previous
51	18	Further, a domain admin was identified that appeared to use a pattern in their BUD password; modifying this pattern ultimately lead to guessing the password for the corresponding DGOZ domain admin account.	The Cyber Security Operations and Analysis Center is much more mature now, this could not take place unnoticed. As well, BPA IT's policy requires much larger passwords of 15 characters or more today, AND we have deployed Multifactor Authentication		see previous
52	19	Some of these network configurations contained Cisco Type 7 password hashes that allowed the attackers to uncover a password that may be reused throughout the environment. As well, multiple versions of the Cisco IOS are in use, many of which appear vulnerable to attack.			see previous
53	19	The malicious Excel file was to be uploaded to the DGOZ file server, and then the main page of one of the webservers modified to prompt the user to open this Excel file.			see previous
54	20	The detection was not reported and the incident response process was not exercised			see previous
55	20	BPA's CISO will prioritize these findings and assign responsibility to the identified roles. Plan of action and milestones (POAM) will be created to ensure BPA's risk is reduced to an acceptable level in a timely manner.			see previous
56					
57					
58					
59					
60					
61					
62					
63					
64					
65					
66					
67					
68					
69					
70					
71					
72					
73					
74					
75					
76					
77					
78					
79					
80					
81					
82					
83					
84					
85					
86					
87					
88					
89					
90					

91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199

From: [Dodd Jr, Gary A \(BPA\) - JB-B1](#)
To: [Collier, Alicia N \(BPA\) - JBC-B1](#); [Jungling, Darren L \(BPA\) - JBC-B1](#); [Callaway III, George M \(BPA\) - JBB-B1](#)
Subject: RE: Tasks
Date: Monday, March 2, 2020 11:27:00 AM

All the high impact IT specific weaknesses were closed during the exercise itself.
Thanks Alicia.

From: Collier, Alicia N (BPA) - JBC-B1 <ancollier@bpa.gov>
Sent: Monday, March 2, 2020 10:56 AM
To: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>; Jungling, Darren L (BPA) - JBC-B1 <dljungling@bpa.gov>; Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>
Subject: RE: Tasks

These are the docs I pulled together last week. The excel spreadsheet has 3 tabs for the POAMs, CCN-RT, FIELD-RT, and BUD-RT. I have added the CCN Red Team closure report that I had written up 3-18-19. I do not have Field or Bud info other than the high level info. Katie had worked with J long ago and I think at one point we had said we were not working on them any longer and to archive.

Let me know if you have any questions. Vicky and I are working on budget info and will have that to you by 3/5/20.

Thank you,

Alicia Collier

Office of Cyber Security | Cyber Security Remediation and Reporting
BONNEVILLE POWER ADMINISTRATION
905 NE 11th Ave | MS: JBB-B1 | Portland, OR 97232
bpa.gov | P 503-230-4485

Thanks,

From: Dodd Jr, Gary A (BPA) - JB-B1 <gadodd@bpa.gov>
Sent: Monday, March 2, 2020 10:37 AM
To: Jungling, Darren L (BPA) - JBC-B1 <dljungling@bpa.gov>; Collier, Alicia N (BPA) - JBC-B1 <ancollier@bpa.gov>; Callaway III, George M (BPA) - JBB-B1 <gmcallaway@bpa.gov>
Subject: FW: Tasks

Number 2 is still outstanding.

I need to get a full accounting of where we are at on that, where we left off and what those items look like today.

From: Dodd Jr, Gary A (BPA) - JB-B1
Sent: Tuesday, February 25, 2020 3:02 PM
To: Jungling, Darren L (BPA) - JBB-B1 <dljungling@bpa.gov>
Subject: Tasks

Darren,

I need some help with a few things and I've not been able to touch base.

1. Melanie has asked for a solid budget forecast for the remainder of FY 2020. We may not spend what we've got
 2. Jon Nichols (I spoke to him briefly) mentioned that there were red team POA&Ms. Now that the report is public we should take a look at where those were left.
- Gary

Control Center Network (CCN) Red Team POAM Remediation Summary

CCN-RedTeam-102014-1

Weakness: File modifications/additions to web servers

- A. Milestone 1 [4-30-17] -Configure Tripwire to monitor root and system files on selected DMZ systems capable of tripwire in order to understand the level of effort and resources needed to improve CCN monitoring capabilities.
 - For the selected DMZ systems
 - Monitor Root C for new files and changes. (Excluding folder changes). Investigate possibility of alerting changes to Splunk.
 - Take a snapshot of system files to quantify amount and noise. Monitor C:/windows/system and system32 on a select DMZ system.
 - Ensure Tripwire is monitoring on the effective systems.
 - In collaboration with JB, Analyze Data to determine acceptable files to be monitored from the selection listed above.
- B. Milestone 2 [6-30-17] - Based on the data gathered, knowledge learned and agreement with JB from above, and current system constraints:
 - Configure Tripwire for monitoring on the all remaining DMZ systems
- C. Milestone 3 [4-30-17] - Configure SPLUNK to receive FIN data.
- D. Milestone 4 [4-30-17] - Configure SPLUNK to receive all CCN network device logs where capable.

Response: Retest CRM2321892. The assessor passed the retest on 10/27/2017.

POAM Status: Complete

CCN-RedTeam-102014-2

Weakness: Many service accounts and user accounts (both regular and elevated) were cracked within 24 hours because they only used 6 characters and a known pattern.

- A. Milestone 1 [4-30-17] - Implement domain GPO for all accounts for 16 character passwords.
- B. Milestone 2 [4-30-17] - Update Windows account management plan to reflect change in standard. (16 character service account passwords.)
- C. Milestone 3 [4-30-17] – Create and enforce Control Center issue-specific password policy.

Response: Retest CRM 2267114. The assessor listed POAM as Complete-Mitigated to Moderate 03/01/17.

Assessor Notes: Sufficient evidence has been provided that string password policies have been implemented and the POA&M has been met. The original weakness identified several recommendations that would help establish a robust password management program. One recommendation (password enforcement) is addressed and remediated through this POA&M. The other elements (user awareness and password monitoring) of the password management weakness constitute a residual risk of Medium.

POAM Status: Complete-Mitigate to Moderate

CCN-RedTeam-102014-3

Weakness: Usage of type 7 passwords for Cisco devices (DGOZ).

- A. Milestone 1 [4-30-17] - Implement MD5 password encryption on all capable network devices within CCN.
- B. Milestone 2 [4-30-17] - Update network account management plan to reflect the MD5 password requirement.
- C. Milestone 3 [4-30-17] – Create and enforce Control Center issue-specific password policy.

Response: Retest CRM 2267182. The assessor passed the retest on 03-10-2017.

POAM Status: Complete

CCN-RedTeam-102014-4

Weakness: Systems failed to detect known malware such as Veil, Invoke-Mimikatz and F-pipe.

- A. Milestone 1 - [07-01-17] - Investigate Host Based IPS for windows systems. Complete Written Proposal.
- B. Milestone 2 - [09-30-17] - Submit Effort for FY18 Capitol Project.

Response: Retest CRM 2267182. A risk acceptance memorandum has been prepared by the ISO with consult and coordination through the information owner (IO). The Remediation Team will work with the CISO for follow-up and presentation to the Authorizing Official. (See Appendix A)

POAM Status: Complete-Residual Risk

CCN-RedTeam-102014-5

Weakness: Domain users from the BUD AD domain were allowed to authenticate into DGOZ. Applications in DGOZ recognize BUD credentials.

- A. Milestone 1 [09-01-17] - Create Project Plan and Proposal for the following:
 - Remove the domain trust from BUD to DGOZ.
 - Design and Implement and DMZ architecture that does not require the BUD.
 - Review the necessity of all ports and services.

Response: Retest CRM 2387744. The assessor failed the retest 03-12-2017.

Assessor Notes: According to the evidence provided, no mitigation or remediation has been accomplished.

POAM Status: Complete-Residual Risk

CCN-RedTeam-102014-6

Weakness: Malicious files were identified, but did not follow cyber security incident response process appropriately.

- A. Milestone 1 - [4-30-17]- Update the Control Center IR Plan.
- B. Milestone 2 - [4-30-17] - Rollout incident Response (IR) Training. Communication and outreach. Add to NERC CIP Training FY17.

Response: Retest CRM 2267191. The assessor passed the retest on 02-23-2017.

POAM Status: Complete

CCN-RedTeam-102014-7

Weakness: Open ports allowed services such as RDP and telnet from BUD network to DGOZ network.

- A. Milestone 1 - [6-30-17]- Update Control Center ESP Plan to show jump host placement.

Response: Retest CRM 2267146. The assessor failed the retest on 03-28-2017.

Assessor Notes: It is unclear how the identified milestones and mitigations protect the CCN DMZ from interactive sessions established from a lower trust zone (BUD). The recommendation was to not allow RDP sessions from BUD to the CCN DMZ. It appears that password-based RDP access to the CCN DMZ is still possible. It is not clear what the requirement is to allow interactive RDP access from BUD to CCN DMZ.

POAM Status: Complete-Residual Risk

CCN-RedTeam-102014-8

Weakness: Several internal scan campaigns were conducted and went undetected:
From BUD network to all known DGOZ network ranges. (Ports 21, 22, 23, 80, 443, 15001)
From DGOZ to all known DGOZ network ranges. (Ports 21, 22, 23, 80, 443, 445, 15001)
From DGOZ to all known DGO network ranges (Ports 21, 22, 23, 80, 443, 445, 15001).

A. Milestone 1 [6-30-17] - Provide a copy of all scan triggers for review. (IDS & Splunk)

Response: Retest CRM 2321903. The remediator closed the retest due to length of time open on 02-02-18.

Remediation Notes: Assessor requested additional information from Transmission regarding port scanning was conducted against the CCN DMZ environment. Transmission provided screenshot of the IDS Internal Intrusion Alert that Triggered to Evidence folder. The assessor still needed more evidence and clarification. Timed out?

POAM Status: Retest Not Complete – Incomplete Data

CCN-RedTeam-102014-9

Weakness: Attackers gain information from LDAP server queries. Initially, these queries tend to be very broad to collect as much information as possible.

A. Milestone 1 [06-30-17] Splunk LDAP Triggers

- Splunk entry that shows event log 1644.
- Provide a description of the trigger from LDAP queries and evidence (event log 1644) in Splunk.
- When implemented for real time, provide copy of screenshot of Splunk alert.

Response: Retest CRM 2321905. The assessor failed the retest on 10-25-2017. Although evidence was submitted regarding the screen shots of Alert Manager, where the alert triggered, as well as an excerpt from the document "Splunk Daily Checks" outlining the CC response to this alert, the assessor did not see the final close loop from their process to notify CSI team of the alert from the assessors retest.

Assessor Notes: According to the evidence provided, broad LDAP queries are unable to be detected at this time.

POAM Status: Complete-Residual Risk

CN-RedTeam-102014-10

Weakness: User account passwords were reused between BUD and DGOZ domains.

A. Milestone 1 [06-30-17] - Enhance password complexity requirements and length on all capable devices or implement PIV.

B. Milestone 2 [06-30-17] – Create and enforce Control Center issue-specific password policy.

Response: Retest CRM 2291167. The CISO passed the retest on 10-02-2017. (George/Darren to find in archive emails?)

Appendix A

Insert Memo Here (sent email to Rustin 3-18-19)

POAM ID	POAM Type	POAM Status	Remediation ID	Designated Milestone Completion Date	POAM Risk Rating	GSS	Assessment Year	Application or System Full Name	ISO	JBB POC	CRM	POAM Creation Date	POAM Complete Date
BUD-RedTeam-102014-1	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-10	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-11	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-12	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-13	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-14	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-15	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-16	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie	2182935	6/14/2016	7/1/2016
BUD-RedTeam-102014-17	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie	2184245	6/14/2016	7/1/2016
BUD-RedTeam-102014-18	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie	2183013	6/14/2016	7/1/2016
BUD-RedTeam-102014-2	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-3	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-4	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie	2183027	6/14/2016	7/1/2016
BUD-RedTeam-102014-5	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
BUD-RedTeam-102014-6	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	6/14/2016
BUD-RedTeam-102014-7	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie	2016095	6/14/2016	3/11/2015
BUD-RedTeam-102014-8	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie	2017226	6/14/2016	4/15/2015
BUD-RedTeam-102014-9	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	GCE	2014	GCE	Buttress, Larry	Feucht, Katie		6/14/2016	7/1/2016
JB-RedTeam-102014-1	Internal Assessment	Complete	BUD-RedTeam-102014		HIGH	Enterprise	2014	Enterprise	Dodd Jr, Gary	Feucht, Katie		6/14/2016	

POAM ID	POAM Type	POAM Status	Remediation ID	Designated Milestone Completion Date	POAM Risk Rating	GSS	Assessment Year	Application or System Full Name	ISO	JBB POC	CRM	POAM Creation Date	POAM Complete Date
FLD-RedTeam-102014-1	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019
FLD-RedTeam-102014-2	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019
FLD-RedTeam-102014-3	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019
FLD-RedTeam-102014-4	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019
FLD-RedTeam-102014-5	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019
FLD-RedTeam-102014-6	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019
FLD-RedTeam-102014-7	Internal Assessment	Complete	FLD-RedTeam-102014		HIGH	FLD	2014	FLD		Collier, Alicia		6/14/2016	2/7/2019

POAM ID	POAM Type	POAM Status	Remediation ID	Designated Milestone Completion Date	POAM Risk Rating	GSS	Assessment Year	Application or System Full Name	ISO	JBB POC	CRM	POAM Creation Date	POAM Complete Date
CCN-RedTeam-102014-01	Internal Assessment	Complete	CCN-RedTeam-102014	6/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	10/25/2017
CCN-RedTeam-102014-02	Internal Assessment	Residual Risk	CCN-RedTeam-102014	4/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	3/10/2017
CCN-RedTeam-102014-03	Internal Assessment	Complete	CCN-RedTeam-102014	4/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	3/10/2017
CCN-RedTeam-102014-04	Internal Assessment	Residual Risk	CCN-RedTeam-102014	9/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	10/25/2017
CCN-RedTeam-102014-05	Internal Assessment	Residual Risk	CCN-RedTeam-102014	9/1/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	10/25/2017
CCN-RedTeam-102014-06	Internal Assessment	Complete	CCN-RedTeam-102014	4/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	2/23/2017
CCN-RedTeam-102014-07	Internal Assessment	Residual Risk	CCN-RedTeam-102014	6/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	6/30/2017
CCN-RedTeam-102014-08	Internal Assessment	Retest	CCN-RedTeam-102014	6/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	10/25/2017
CCN-RedTeam-102014-09	Internal Assessment	Residual Risk	CCN-RedTeam-102014	6/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	10/25/2017
CCN-RedTeam-102014-10	Internal Assessment	Complete	CCN-RedTeam-102014	6/30/2017	HIGH	CCS	2014	CNN-Red Team	Ngo, Huy	Collier, Alicia	NA	2/21/2017	10/2/2017

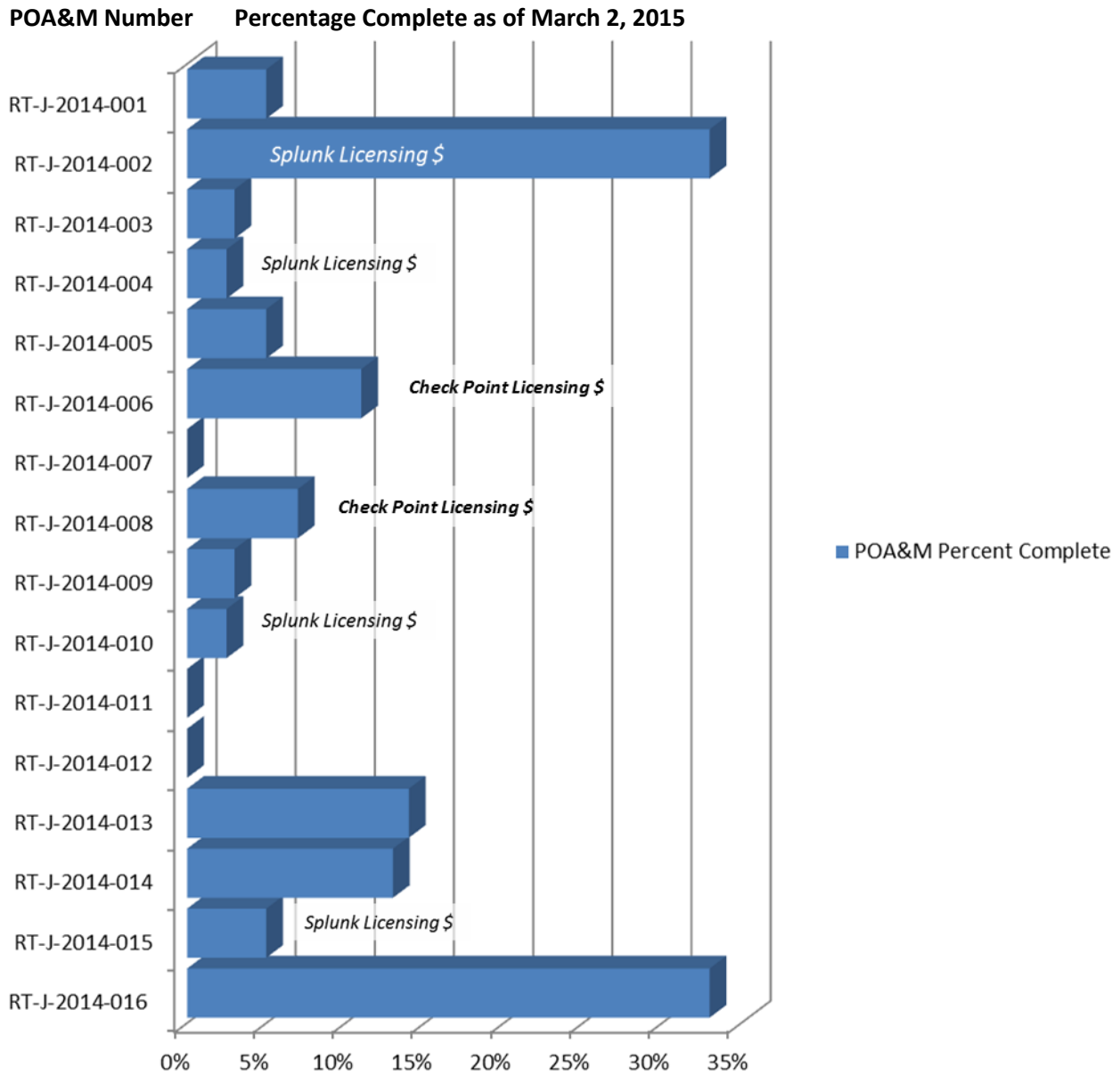
Red Team Vulnerability Remediation Report

The graph below represents the amount of remediation work completed for each of the findings detailed in Cyber Security's Red Team Security Assessment Report (SAR) dated December 2014.

This report also illustrates which findings or POA&Ms immediate funding requests for the **Check Point Firewall License Upgrade** and **Splunk Exchange App Licensing** will address.

The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

POA&M Percent Complete



POA&M Details

RT-J-2014-001	Audit and Accountability - Access: Undetected File Modification
RT-J-2014-002	Audit and Accountability - Access: Undetected malicious execution
RT-J-2014-003	Audit and Accountability - Undetected Internal Service and Port Scans
RT-J-2014-004	Audit and Accountability - Undetected LDAP Queries of Active Directory
RT-J-2014-005	Access Control - System and Communication Protection: Writeable Startup Folders for "All Users" and individual user
RT-J-2014-006	System and Communication Protection - Successful modification of MS workstation firewall, allowing opening of local ports
RT-J-2014-007	System and Communication Protection: Port and vulnerability scans undetected
RT-J-2014-008	System and Communication Protection: Protocol/port mismatches outbound through external firewalls
RT-J-2014-009	System and Communication Protection: Malware not detected
RT-J-2014-010	System Information Integrity - Email Address Spoofing on external BPA SMTP servers
RT-J-2014-011	System Information Integrity - SPAM filter can be modified to allow blocked IPs
RT-J-2014-012	System Information Integrity - Excel files with malicious macros not blocked
RT-J-2014-013	Configuration Management: Workstation configuration not standardized allowing successful attacks
RT-J-2014-014	Configuration Management: Password policies not consistent across accounts
RT-J-2014-015	Audit and Accountability: Log content not complete or tuned
RT-J-2014-016	System and Communication Protection Access Control: Domain trusts and network traffic not well documented

Funding Requests for Licensing

- **Check Point Firewall License Upgrade - \$200,000**

This upgrade will allow all 12 cores on Check Point firewalls to run. Currently, only 4 cores are running. This upgrade will allow all the functionality without being limited by current processor constraints.

- **Splunk Exchange App Licensing - \$60,000**

This request will cover the Splunk Exchange App and licensing for Exchange server logging in all environments.

Red Team Vulnerability Remediation Report

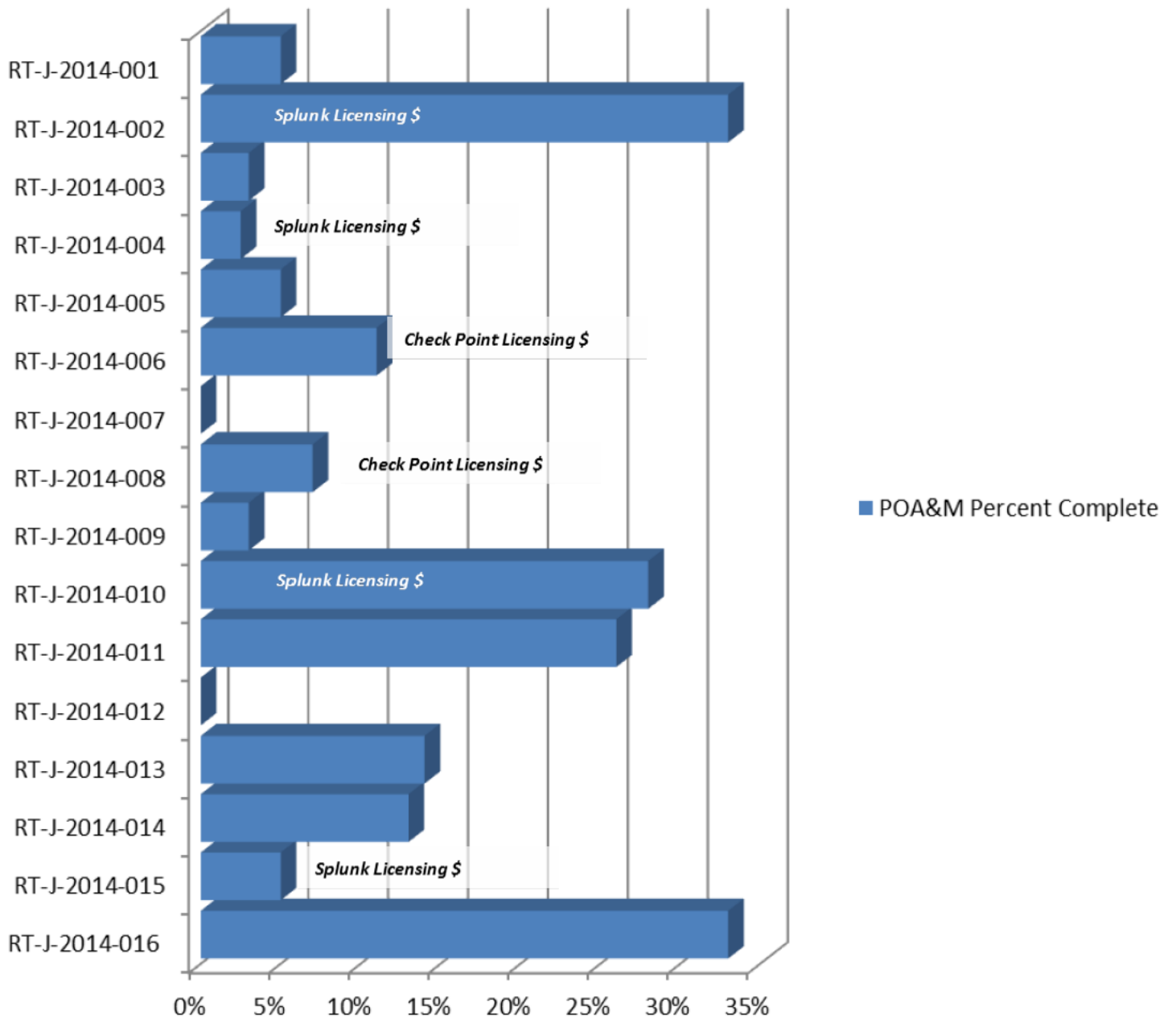
The graph below represents the amount of remediation work completed for each of the findings detailed in Cyber Security's Red Team Security Assessment Report (SAR) dated December 2014.

This report also illustrates which findings or POA&Ms immediate funding requests for the *Check Point Firewall License Upgrade* and *Splunk Exchange App Licensing* will address.

The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

POA&M Percent Complete

POA&M Number Percentage Complete as of March 4, 2015



POA&M Details

RT-J-2014-001	Audit and Accountability - Access: Undetected File Modification
RT-J-2014-002	Audit and Accountability - Access: Undetected malicious execution
RT-J-2014-003	Audit and Accountability - Undetected Internal Service and Port Scans
RT-J-2014-004	Audit and Accountability - Undetected LDAP Queries of Active Directory
RT-J-2014-005	Access Control - System and Communication Protection: Writeable Startup Folders for "All Users" and individual user
RT-J-2014-006	System and Communication Protection - Successful modification of MS workstation firewall, allowing opening of local ports
RT-J-2014-007	System and Communication Protection: Port and vulnerability scans undetected
RT-J-2014-008	System and Communication Protection: Protocol/port mismatches outbound through external firewalls
RT-J-2014-009	System and Communication Protection: Malware not detected
RT-J-2014-010	System Information Integrity - Email Address Spoofing on external BPA SMTP servers
RT-J-2014-011	System Information Integrity - SPAM filter can be modified to allow blocked IPs
RT-J-2014-012	System Information Integrity - Excel files with malicious macros not blocked
RT-J-2014-013	Configuration Management: Workstation configuration not standardized allowing successful attacks
RT-J-2014-014	Configuration Management: Password policies not consistent across accounts
RT-J-2014-015	Audit and Accountability: Log content not complete or tuned
RT-J-2014-016	System and Communication Protection Access Control: Domain trusts and network traffic not well documented

Funding Requests for Licensing

- **Check Point Firewall License Upgrade - \$200,000**

This upgrade will allow all 12 cores on Check Point firewalls to run. Currently, only 4 cores are running. This upgrade will allow all the functionality without being limited by current processor constraints.

- **Splunk Exchange App Licensing - \$60,000**

This request will cover the Splunk Exchange App and licensing for Exchange server logging in all environments.

Funding Requests for Licensing

- **Check Point Firewall License Upgrade - \$200,000**

This upgrade will allow all 12 cores on Check Point firewalls to run. Currently, only 4 cores are running. This upgrade will allow all the functionality without being limited by current processor constraints.

- **Splunk Exchange App Licensing - \$60,000**

This request will cover the Splunk Exchange App and licensing for Exchange server logging in all environments.

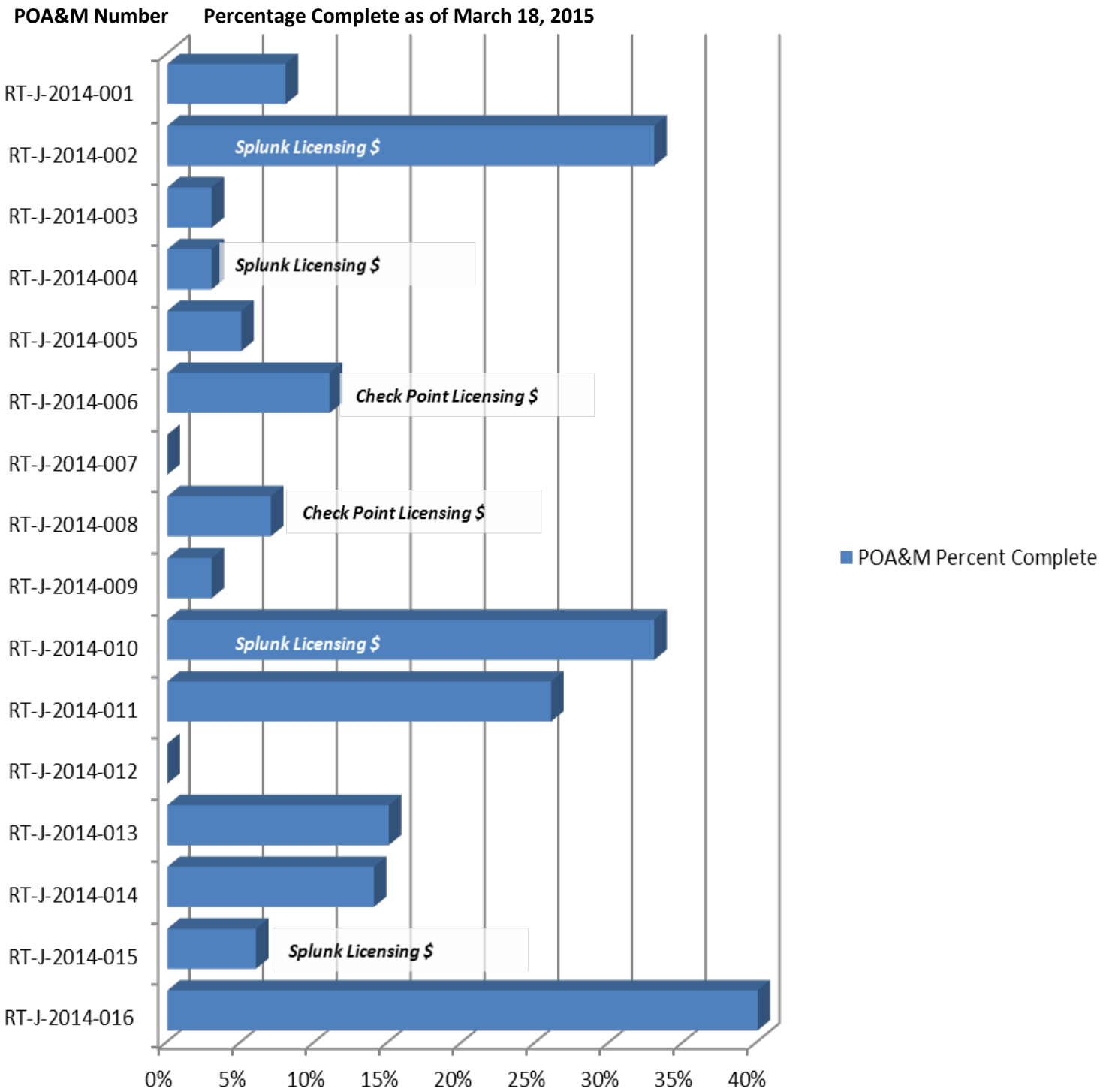
Red Team Vulnerability Remediation Report

The graph below represents the amount of remediation work completed for each of the findings detailed in Cyber Security's Red Team Security Assessment Report (SAR) dated December 2014.

This report also illustrates which findings or POA&Ms immediate funding requests for the ***Check Point Firewall License Upgrade*** and ***Splunk Exchange App Licensing*** will address.

The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

POA&M Percent Complete



POA&M Details

RT-J-2014-001	Audit and Accountability - Access: Undetected File Modification
RT-J-2014-002	Audit and Accountability - Access: Undetected malicious execution
RT-J-2014-003	Audit and Accountability - Undetected Internal Service and Port Scans
RT-J-2014-004	Audit and Accountability - Undetected LDAP Queries of Active Directory
RT-J-2014-005	Access Control - System and Communication Protection: Writeable Startup Folders for "All Users" and individual user
RT-J-2014-006	System and Communication Protection - Successful modification of MS workstation firewall, allowing opening of local ports
RT-J-2014-007	System and Communication Protection: Port and vulnerability scans undetected
RT-J-2014-008	System and Communication Protection: Protocol/port mismatches outbound through external firewalls
RT-J-2014-009	System and Communication Protection: Malware not detected
RT-J-2014-010	System Information Integrity - Email Address Spoofing on external BPA SMTP servers
RT-J-2014-011	System Information Integrity - SPAM filter can be modified to allow blocked IPs
RT-J-2014-012	System Information Integrity - Excel files with malicious macros not blocked
RT-J-2014-013	Configuration Management: Workstation configuration not standardized allowing successful attacks
RT-J-2014-014	Configuration Management: Password policies not consistent across accounts
RT-J-2014-015	Audit and Accountability: Log content not complete or tuned
RT-J-2014-016	System and Communication Protection Access Control: Domain trusts and network traffic not well documented

Funding Requests for Licensing

- **Check Point Firewall License Upgrade - \$200,000**

This upgrade will allow all 12 cores on Check Point firewalls to run. Currently, only 4 cores are running. This upgrade will allow all the functionality without being limited by current processor constraints.

- **Splunk Exchange App Licensing - \$60,000**

This request will cover the Splunk Exchange App and licensing for Exchange server logging in all environments.

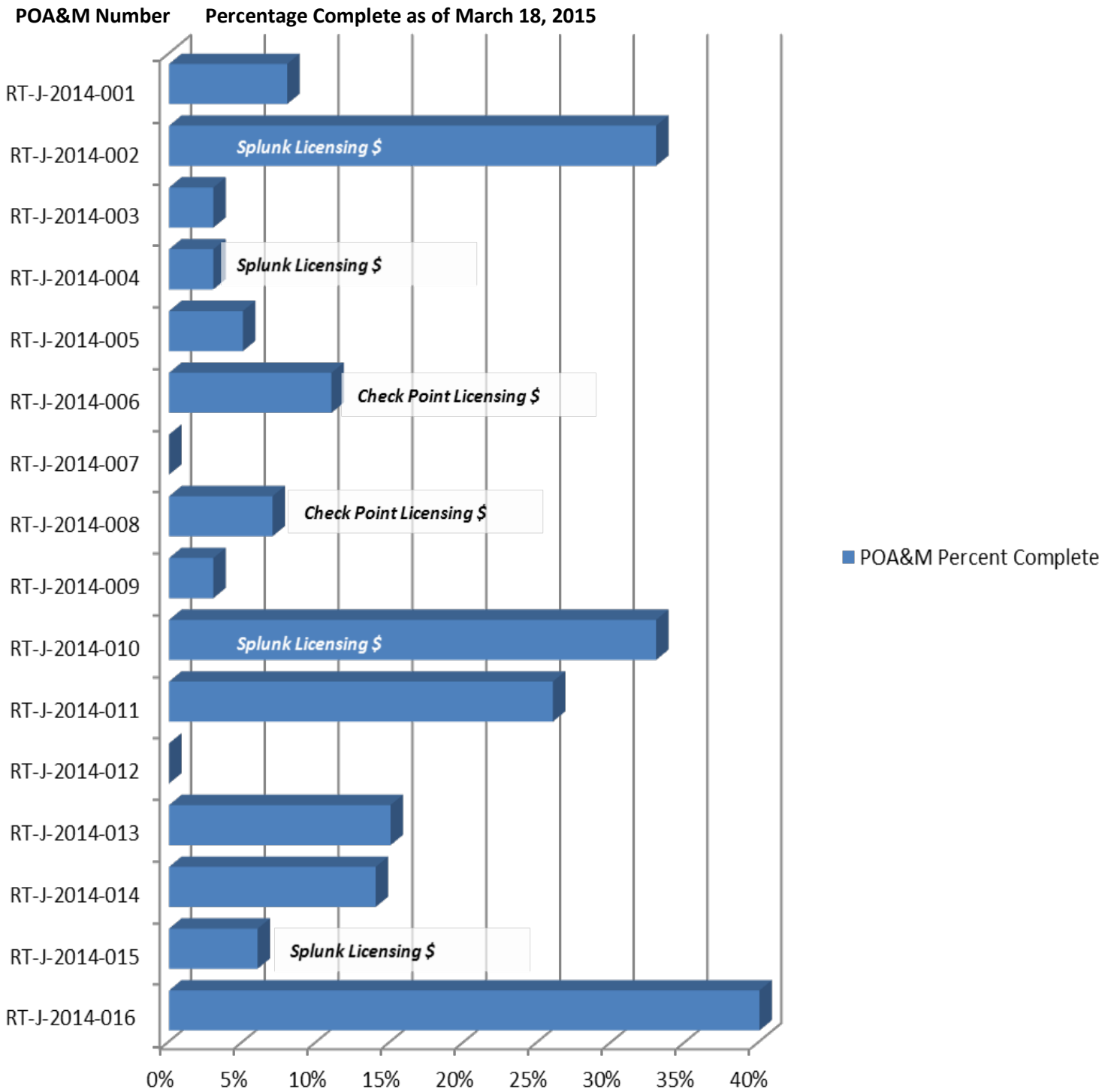
Red Team Vulnerability Remediation Report

The graph below represents the amount of remediation work completed for each of the findings detailed in Cyber Security's Red Team Security Assessment Report (SAR) dated December 2014.

This report also illustrates which findings or POA&Ms immediate funding requests for the ***Check Point Firewall License Upgrade*** and ***Splunk Exchange App Licensing*** will address.

The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

POA&M Percent Complete



POA&M Details

POA&M

Remediation Tasks

(some tasks span multiple POA&Ms)

RT-J-2014-001	Remove Unnecessary users from admin groups; Update scripts for lan.bat creation; Update lan.bat permissions; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Remove unused lan.bat legacy settings; Develop automated asset inventory to allow monitoring of new systems; Choose technology for drive mapping solutions; Evaluate <i>File Integrity Monitoring</i> (FIM) implementation; Choose technologies for FIM solution; Complete list of high risk systems
RT-J-2014-002	Evaluate implementation of AppLocker temp directory; Choose technology for temp directory whitelisting; Evaluate implementation of EndPoint Protection; Choose technology for EndPoint Protection Solution; Verify that myPC servers are sending logs to Splunk; Evaluate implementation for logging at endpoints; Choose technology for endpoint logging; Complete process for leveraging workstation logs as part of event monitoring; Complete list of high risk systems; Determine <i>end of life</i> (EOL) of Forefront;
RT-J-2014-003	Renew contract and review support for Cisco <i>Network Intrusion Detection System</i> (NIDS); Work with CSOAC on NIDS feeds to Splunk; Evaluate implementation of NIDS; Choose NIDS technology; Ensure new NIDS logs are ingested by Splunk; Ensure NIDS logs response procedures are in place; Evaluate implementation of Splunk <i>Enterprise Security</i> (ES); Determine EOL of Forefront
RT-J-2014-004	Cleanup descriptions of <i>Elevated Privileges User</i> (EPU) accounts; Build Domain Admin servers and workstations; Configure domain controllers to log LDAP events to Splunk;
RT-J-2014-005	Implement FIM including logging; AppLocker Implementation; Determine EOL of Forefront; Implement endpoint protection suite incorporating application whitelisting;
RT-J-2014-006	Determine EOL of Forefront; Implement endpoint protection suite incorporating application whitelisting; Update Application Control DB on <i>firewalls</i> (FWs); Remove unnecessary ports from the internal IPs to external IPs FW rule; Upgrade Check Point FWs to most recent version, renew contract; Replace perimeter Check Point FWs; Cleanup Citrix group policies; Cleanup workstation group policies; Configure <i>Web Cache Communications Protocol</i> (WCCP) for myPC forcing web traffic through WebSense; Upgrade WebSense; Select and implement Web Proxy to replace EoL for WebSense
RT-J-2014-007	Investigate <i>Data Loss Prevention</i> (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; Review Cisco support contract for NIDS, ensuring receipt of new

signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Replace NIDS equipment; Evaluate implementation of Splunk ES; Implement a Web Application FW;

RT-J-2014-008	Remove unnecessary ports from internal IP to external IP FW rules; Upgrade Check Point FWs and renew contract; Renew Cisco contract for NIDS ensure receipt of new signatures; Ensure CSOAC receives proper NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Replace NIDS equipment; Implement Splunk ES; Configure WCCP to ensure web traffic from myPC goes through WebSense; Upgrade WebSense; Replace EoL WebSense;
RT-J-2014-009	Investigate EoL for Forefront; Implement EndPoint protection incorporating Application Whitelisting; Renew Cisco contract for NIDS, ensuring receipt of new signatures; Replace NIDS equipment; Implement Splunk ES
RT-J-2014-010	Ensure Exchange sends logs to Splunk; Full review of Exchange environment; Create Exchange Baseline; Implement Exchange mail store malware protection; Prevent external spoofing bpa.gov email addresses; Ensure Sophos receives regular virus definition updates; Ensure Splunk receives Sophos logs;
RT-J-2014-011	Investigate WebSense DLP and Email modules; Replace Sophos equipment; Review Sophos Whitelisting;
RT-J-2014-012	Update group policies for Office product macros
RT-J-2014-013	Tighten group policy change control procedures; Clean up Citrix group policies; Cleanup workstation group policies; Improve management of SPC laptops; Configure WCCP to force web traffic from myPC network through WebSense; Upgrade WebSense; Implement Web Proxy to replace EoLWebSense
RT-J-2014-014	Update weak passwords; Implement password policies for EPU and service accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts
RT-J-2014-015	Coordinate with CSOAC to resolve logging problems; Implement automated inventory of authorized and unauthorized devices
RT-J-2014-016	Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Evaluate and document domain trusts and FW rules between various environments; Implement new FW rule configurations

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.

- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **Ian.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Funding Requests for Licensing

- **Splunk Exchange App Licensing - \$60,000**

This request will cover the Splunk Exchange App and licensing for Exchange server logging in all environments.

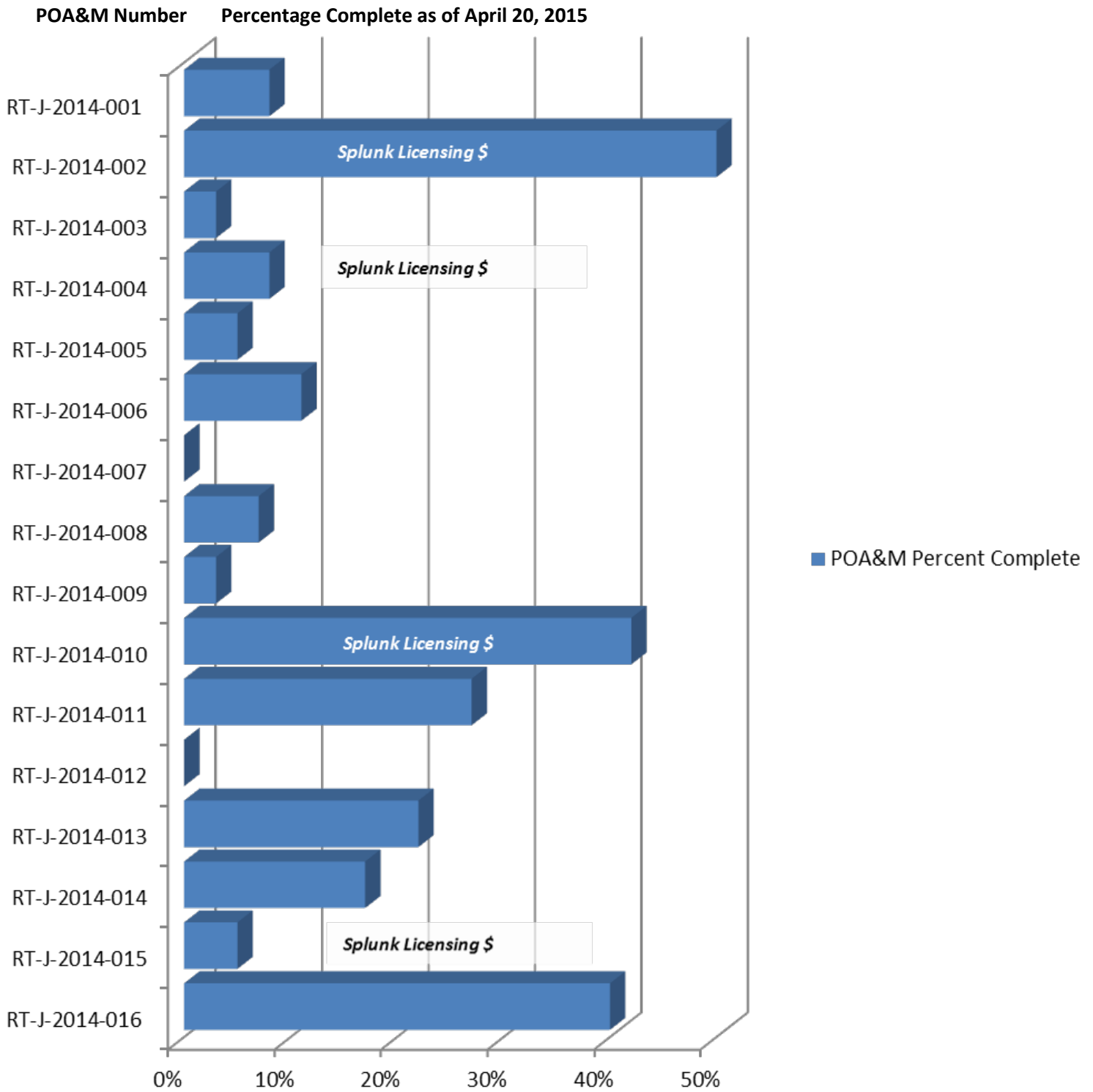
Red Team Vulnerability Remediation Report

The graph below represents the amount of remediation work completed for each of the findings detailed in Cyber Security's Red Team Security Assessment Report (SAR) dated December 2014.

This report also illustrates which findings or POA&Ms immediate funding requests for the ***Splunk Exchange App Licensing*** will address.

The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

POA&M Percent Complete



POA&M Details

POA&M

Remediation Tasks

(some tasks span multiple POA&Ms)

RT-J-2014-001

Work Completed:

Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Remove unused lan.bat legacy settings; Update lan.bat permissions

Work in Progress:

Remove Unnecessary users from admin groups

Work not Started:

Choose technology for drive mapping solutions

Work Scheduled to Begin Later:

Choose technologies for FIM solution; Complete list of high risk systems; Develop automated asset inventory to allow monitoring of new systems; Evaluate *File Integrity Monitoring* (FIM) implementation

RT-J-2014-002

Work Completed:

Evaluate implementation of AppLocker temp directory; Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor specification; Operations staff interviews with vendors

Work in Progress:

Choose technology for EndPoint Protection Solution

Work not Started:

Choose technology for temp directory whitelisting

Work Scheduled to Begin Later:

Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; Complete list of high risk systems

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Ensure new NIDS logs are ingested by Splunk

Work in Progress:

Renew contract and review support for Cisco *Network Intrusion Detection System* (NIDS); Evaluate implementation of Splunk *Enterprise Security* (ES)

Work not Started:

Choose NIDS technology; Ensure NIDS logs response procedures are in place

RT-J-2014-004**Work Completed:**

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk

RT-J-2014-005**Work Completed:**

Requirements gathering for endpoint protection

Work Scheduled to Begin Later:

Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting

RT-J-2014-006**Work Completed:**

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense;

Work in Progress:

Upgrade Check Point FWs to most recent version; Cleanup workstation group policies; Cleanup Citrix group policies

Work Scheduled to Begin Later:

Replace perimeter Check Point FWs; Implement endpoint protection suite incorporating application whitelisting; Upgrade WebSense; Select and implement Web Proxy to replace EoL for WebSense

RT-J-2014-007**Work Complete:**

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk;

Work Scheduled to Begin Later:

Investigate *Data Loss Prevention* (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; Replace NIDS equipment; Evaluate implementation of Splunk ES; Implement a Web Application FW;

RT-J-2014-008**Work Completed:**

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Ensure CSOAC receives proper NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense

Work in Progress:

Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Upgrade WebSense; Replace EoL WebSense

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures

Work in Progress:

Implement Splunk ES

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; Replace NIDS equipment

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos. ;Ensure Exchange sends logs to Splunk;

Work in Progress:

Full review of Exchange environment; Create Exchange Baseline;

Work Scheduled to Begin Later:

Implement Exchange mail store malware protection

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway

Work in Progress:

Currently investigating Sophos logging functionality

Work Scheduled to Begin Later:

Investigate WebSense DLP and Email modules; Make decisions on technology for email gateway solution; Replace Sophos equipment;

RT-J-2014-012

Work Scheduled to Begin Later:

Update group policies for Office product macros

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense;

Work in Progress:

Tighten group policy change control procedures; Cleanup workstation group

policies; Improve management of SPC laptops; Currently performing cleanup in IVC DRE (development domain); Clean up Citrix group policies

Work Scheduled to Begin Later:

Upgrade WebSense; Implement Web Proxy to replace EoLWebSense

RT-J-2014-014

Work Complete:

Update weak passwords

Work in Progress:

Implement password policies for EPU and service accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives;"
Implement automated inventory of authorized and unauthorized devices

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Funding Requests for Licensing

- **Splunk Exchange App Licensing - \$60,000**

This request will cover the Splunk Exchange App and licensing for Exchange server logging in all environments.

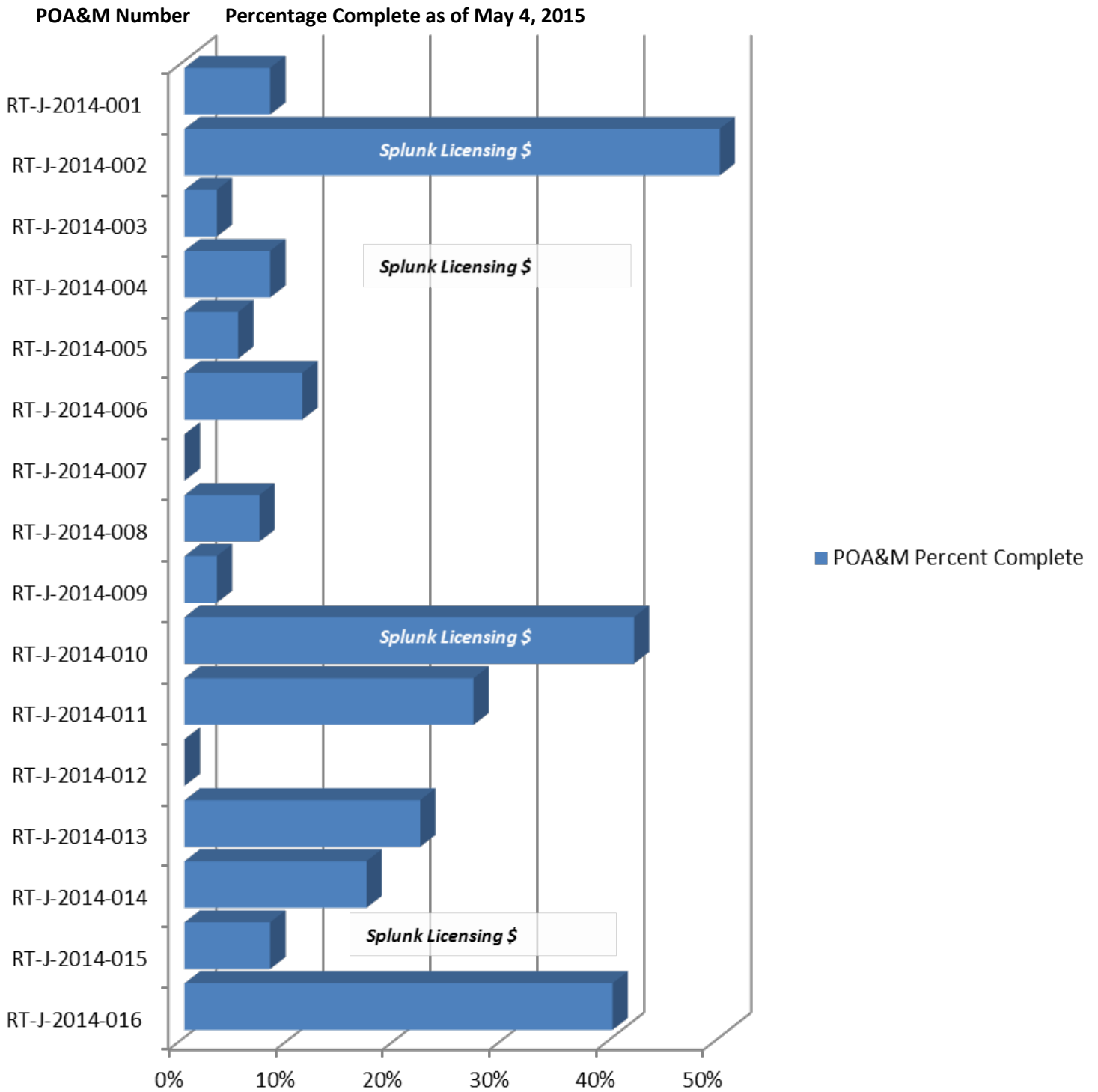
Red Team Vulnerability Remediation Report

The graph below represents the amount of remediation work completed for each of the findings detailed in Cyber Security's Red Team Security Assessment Report (SAR) dated December 2014.

This report also illustrates which findings or POA&Ms immediate funding requests for the ***Splunk Exchange App Licensing*** will address.

The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

POA&M Percent Complete



POA&M Details

POA&M

Remediation Tasks

(some tasks span multiple POA&Ms)

RT-J-2014-001

Work Completed:

Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Remove unused lan.bat legacy settings; Update lan.bat permissions

Work in Progress:

Remove Unnecessary users from admin groups

Work not Started:

Choose technology for drive mapping solutions

Work Scheduled to Begin Later:

Choose technologies for FIM solution; Complete list of high risk systems; Develop automated asset inventory to allow monitoring of new systems; Evaluate *File Integrity Monitoring* (FIM) implementation

RT-J-2014-002

Work Completed:

Evaluate implementation of AppLocker temp directory; Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor specification; Operations staff interviews with vendors

Work in Progress:

Choose technology for EndPoint Protection Solution

Work not Started:

Choose technology for temp directory whitelisting

Work Scheduled to Begin Later:

Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; Complete list of high risk systems

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Ensure new NIDS logs are ingested by Splunk

Work in Progress:

Renew contract and review support for Cisco *Network Intrusion Detection System* (NIDS); Evaluate implementation of Splunk *Enterprise Security* (ES)

Work not Started:

Choose NIDS technology; Ensure NIDS logs response procedures are in place

RT-J-2014-004**Work Completed:**

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk

RT-J-2014-005**Work Completed:**

Requirements gathering for endpoint protection

Work Scheduled to Begin Later:

Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting

RT-J-2014-006**Work Completed:**

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense;

Work in Progress:

Upgrade Check Point FWs to most recent version; Cleanup workstation group policies; Cleanup Citrix group policies

Work Scheduled to Begin Later:

Replace perimeter Check Point FWs; Implement endpoint protection suite incorporating application whitelisting; Upgrade WebSense; Select and implement Web Proxy to replace EoL for WebSense

RT-J-2014-007**Work Complete:**

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk;

Work Scheduled to Begin Later:

Investigate *Data Loss Prevention* (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; Replace NIDS equipment; Evaluate implementation of Splunk ES; Implement a Web Application FW;

RT-J-2014-008**Work Completed:**

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Ensure CSOAC receives proper NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense

Work in Progress:

Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Upgrade WebSense; Replace EoL WebSense

RT-J-2014-009**Work Complete:**

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures

Work in Progress:

Implement Splunk ES

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; Replace NIDS equipment

RT-J-2014-010**Work Complete:**

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos. ;Ensure Exchange sends logs to Splunk;

Work in Progress:

Full review of Exchange environment; Create Exchange Baseline;

Work Scheduled to Begin Later:

Implement Exchange mail store malware protection

RT-J-2014-011**Work Complete:**

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway

Work in Progress:

Currently investigating Sophos logging functionality

Work Scheduled to Begin Later:

Investigate WebSense DLP and Email modules; Make decisions on technology for email gateway solution; Replace Sophos equipment;

RT-J-2014-012**Work Scheduled to Begin Later:**

Update group policies for Office product macros

RT-J-2014-013**Work Completed:**

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense;

Work in Progress:

Tighten group policy change control procedures; Cleanup workstation group

policies; Improve management of SPC laptops; Currently performing cleanup in IVC DRE (development domain); Clean up Citrix group policies

Work Scheduled to Begin Later:

Upgrade WebSense; Implement Web Proxy to replace EoLWebSense

RT-J-2014-014

Work Complete:

Update weak passwords

Work in Progress:

Implement password policies for EPU and service accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives;"
Implement automated inventory of authorized and unauthorized devices

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising our mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team's objectives were BPA's mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Percentages Complete

The graph below represents the amount of remediation work completed for each POA&M on a particular date.

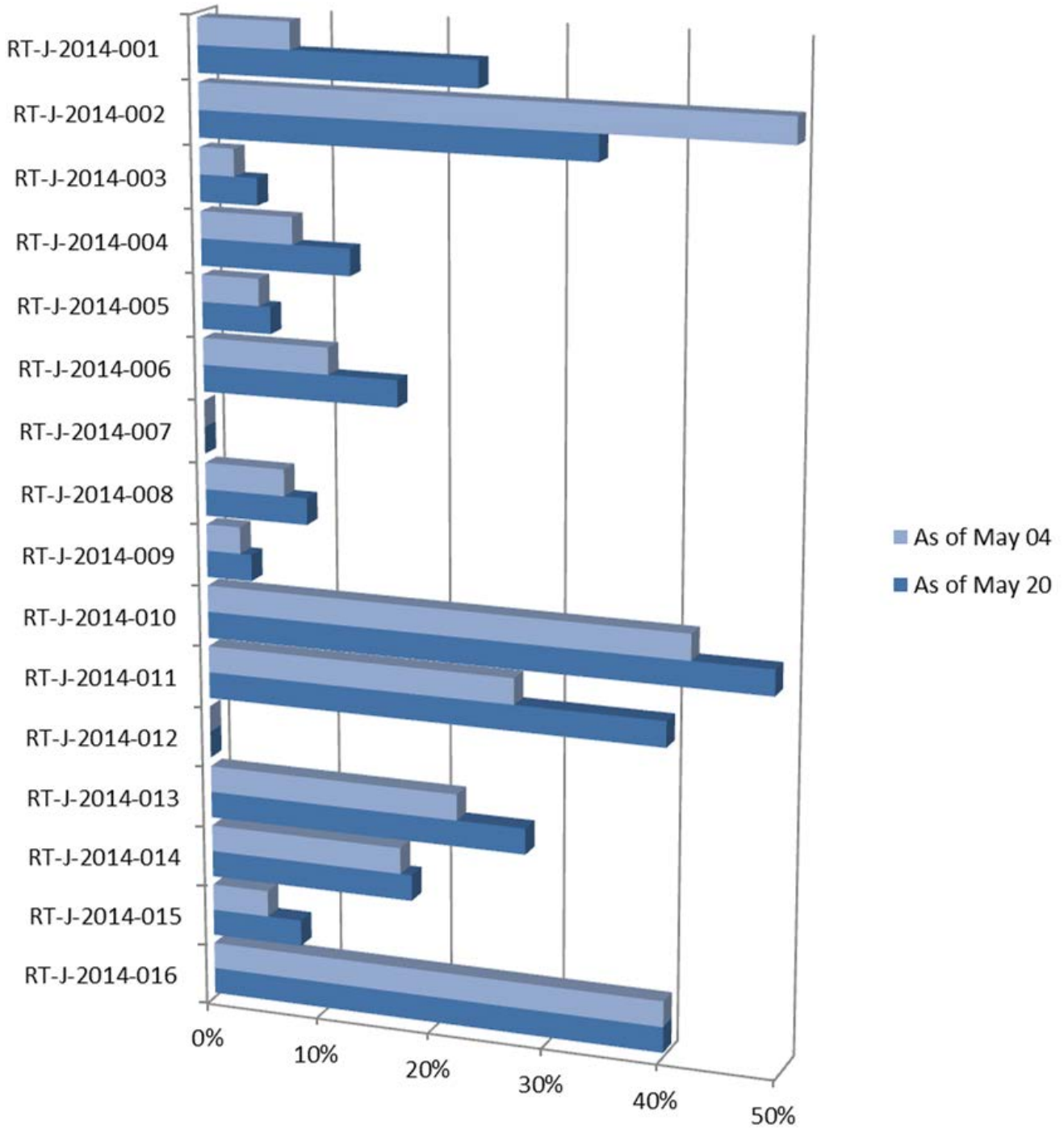
The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

Each percentage complete is represented by two bars. In order to illustrate the amount of progress made since the last report was issued, the *percent complete* is shown for the previous report as well.

The section appearing below the graph outlines each POAM, and divides tasks into those that are *Complete*, *In Progress*, *Not Started*, and *Scheduled to Begin at a Later Date*.

POA&M Percent Complete

POA&M Number Percentage Complete as of June 1, 2015



POA&M Details

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M

Remediation Tasks

(some tasks address multiple POA&Ms)

RT-J-2014-001

Work Completed:

Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Remove unused lan.bat legacy settings; Update lan.bat permissions; Drive mapping solution is chosen (staying with lan.bat for primary drive mapping purposes)

Work in Progress:

Remove Unnecessary users from admin groups; Team is reviewing 37 other unique .bat files called within lan.bat; Cleaning up legacy calls.

Work Scheduled to Begin Later:

Choose technologies for FIM solution; Complete list of high risk systems; Develop automated asset inventory to allow monitoring of new systems; Evaluate *File Integrity Monitoring* (FIM) implementation

RT-J-2014-002

Work Completed:

Evaluate implementation of AppLocker temp directory; Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Choose technology for EndPoint Protection Solution; installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work not Started:

Choose technology for temp directory whitelisting

Work Scheduled to Begin Later:

Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; Complete list of high risk systems

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Ensure new NIDS logs are ingested by Splunk; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Renew contract and review support for Cisco *Network Intrusion Detection System* (NIDS); Evaluate implementation of Splunk *Enterprise Security* (ES); installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work not Started:

Requirements gathering for NIDS technology; **Choose NIDS technology; Finish NIDS system planning phase and submit staffing plan and request for funds; Document O&M requirements for NIDS solution; Ensure NIDS logs response procedures are in place;**

RT-J-2014-004**Work Completed:**

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

RT-J-2014-005**Work Completed:**

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Installation of TrendMicro software in DRE for testing; ; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting

RT-J-2014-006**Work Completed:**

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded.

Work in Progress:

Changes to draft updated Windows 7 standard; Upgrade Check Point FWs to most recent version; Cleanup workstation group policies; Cleanup Citrix group policies; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Replace perimeter Check Point FWs; Implement endpoint protection suite incorporating application whitelisting; Upgrade WebSense; Select and implement Web Proxy to replace EoL for WebSense

RT-J-2014-007**Work Complete:**

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk;

Work Scheduled to Begin Later:

Investigate *Data Loss Prevention* (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; **Replace NIDS equipment**; Evaluate implementation of Splunk ES; Implement a Web Application FW;

RT-J-2014-008**Work Completed:**

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Ensure CSOAC receives proper NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; Core license upgrade received and successfully installed. HQ firewalls are successfully upgraded.

Work in Progress:

Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Upgrade WebSense; Replace EoL WebSense

RT-J-2014-009**Work Complete:**

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Implement Splunk ES; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; **Replace NIDS equipment**

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows

Work in Progress:

Full review of Exchange environment; Exchange baseline monitoring for Tripwire in DRE is ongoing; Purchasing Exchange App for Splunk (contract sent to vendor)

Work Scheduled to Begin Later:

Implement Exchange mail store malware protection

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management

Work in Progress:

Currently investigating Sophos logging functionality

Work not Started:

Finish system planning phase and submit staffing plan and request for funds for email gateway solution; Document O&M requirements for email gateway; Decision on technology for email gateway solution; Complete Sophos replacement project

Work Scheduled to Begin Later:

Investigate WebSense DLP and Email modules; Make decisions on technology for email gateway solution; Replace Sophos equipment;

RT-J-2014-012

Work Scheduled to Begin Later:

Update group policies for Office product macros

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked;

Work in Progress:

Evaluating SPC Admin group rights; Changes to draft updated Windows 7 standard; Improve management of SPC laptops; Currently performing cleanup in IVC DRE (development domain); Clean up Citrix group policies

Work not Started:

Enforce group policy change control policies and procedures

Work Scheduled to Begin Later:

Upgrade WebSense; Implement Web Proxy to replace EoLWebSense

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE

Work in Progress:

Full push of policy in DRE; Implement password policies for EPU and service accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives;"
Implement automated inventory of authorized and unauthorized devices

Work not Started:

Identify staffing plan and implement process for resolution of future logging support.

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising our mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team's objectives were BPA's mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Percentages Complete

The graph below represents the amount of remediation work completed for each POA&M on a particular date.

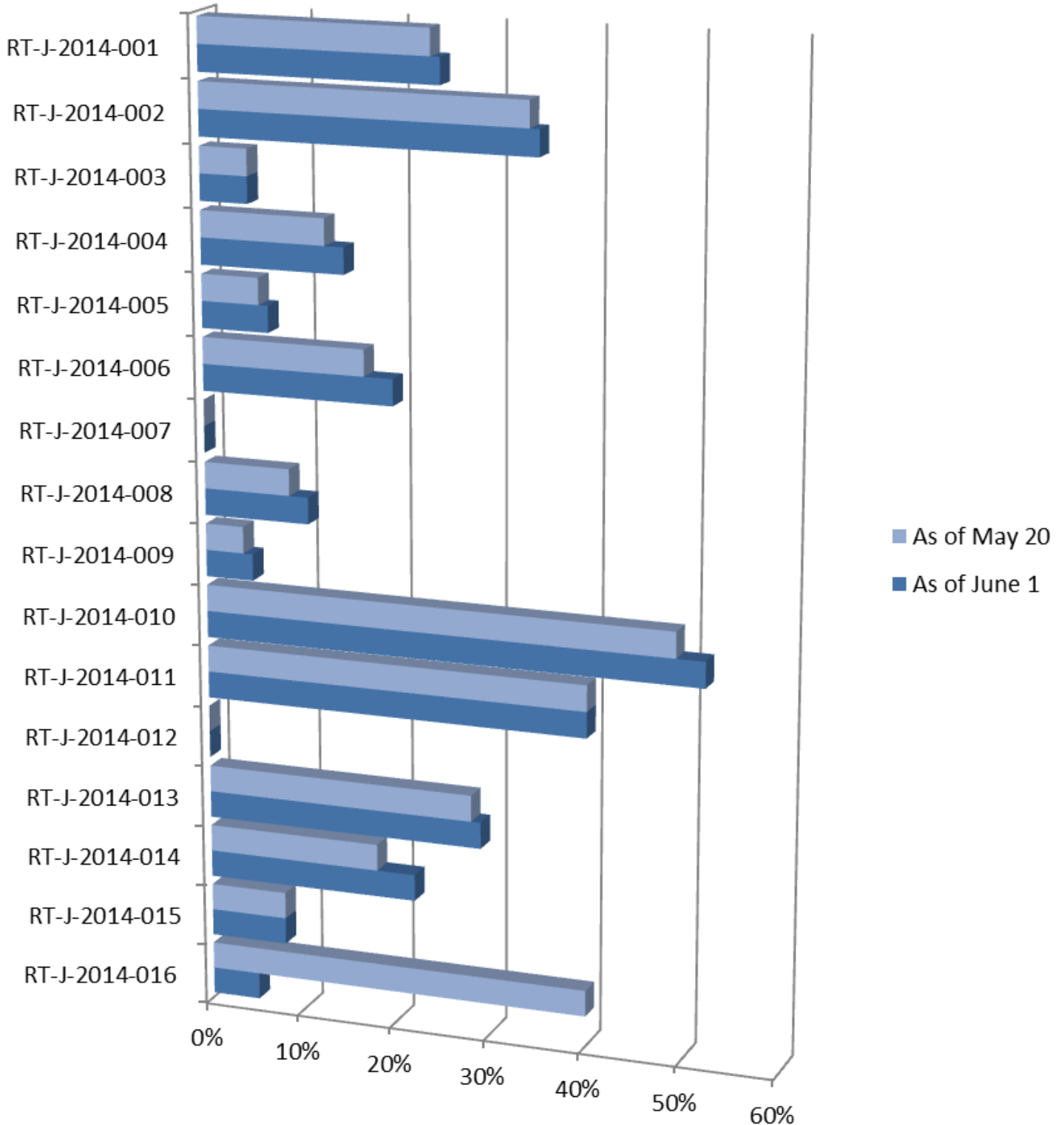
The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

Each percentage complete is represented by two bars. In order to illustrate the amount of progress made since the last report was issued, the *percent complete* is shown for the previous report as well.

The section appearing below the graph outlines each POAM, and divides tasks into those that are *Complete*, *In Progress*, *Not Started*, and *Scheduled to Begin at a Later Date*.

POA&M Percent Complete

POA&M Number Percentage Complete as of June 1, 2015: *Note, RT-J-2014-016 was re-evaluated and a new strategy is being developed.*



POA&M Details

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M

Remediation Tasks

(some tasks address multiple POA&Ms)

RT-J-2014-001

Work Completed:

Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Remove unused lan.bat legacy settings; Update lan.bat permissions; Drive mapping solution is chosen (staying with lan.bat for primary drive mapping purposes)

Work in Progress:

Remove Unnecessary users from admin groups; Team is reviewing 37 other unique .bat files called within lan.bat; Cleaning up legacy calls.

Work Scheduled to Begin Later:

Choose technologies for FIM solution; Complete list of high risk systems; Develop automated asset inventory to allow monitoring of new systems; Evaluate *File Integrity Monitoring* (FIM) implementation

RT-J-2014-002

Work Completed:

Evaluate implementation of AppLocker temp directory; Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Choose technology for EndPoint Protection Solution; installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work not Started:

Choose technology for temp directory whitelisting

Work Scheduled to Begin Later:

Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; Complete list of high risk systems

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Ensure new NIDS logs are ingested by Splunk; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Renew contract and review support for Cisco *Network Intrusion Detection System (NIDS)*; Evaluate implementation of Splunk *Enterprise Security (ES)*; installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work not Started:

Requirements gathering for NIDS technology; **Choose NIDS technology; Finish NIDS system planning phase and submit staffing plan and request for funds; Document O&M requirements for NIDS solution; Ensure NIDS logs response procedures are in place;**

RT-J-2014-004**Work Completed:**

Cleanup descriptions of *Elevated Privileges User (EPU)* accounts; Logging level increased

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

RT-J-2014-005**Work Completed:**

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Installation of TrendMicro software in DRE for testing; ; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting

RT-J-2014-006**Work Completed:**

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls (FWs)*; Configure *Web Cache Communications Protocol (WCCP)* for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded.

Work in Progress:

Changes to draft updated Windows 7 standard; Upgrade Check Point FWs to most recent version; Cleanup workstation group policies; Cleanup Citrix group policies; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Replace perimeter Check Point FWs; Implement endpoint protection suite incorporating application whitelisting; Upgrade WebSense; Select and implement Web Proxy to replace EoL for WebSense

RT-J-2014-007**Work Complete:**

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk;

Work Scheduled to Begin Later:

Investigate *Data Loss Prevention* (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; **Replace NIDS equipment**; Evaluate implementation of Splunk ES; Implement a Web Application FW;

RT-J-2014-008**Work Completed:**

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Ensure CSOAC receives proper NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; Core license upgrade received and successfully installed. HQ firewalls are successfully upgraded.

Work in Progress:

Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Upgrade WebSense; Replace EoL WebSense

RT-J-2014-009**Work Complete:**

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Implement Splunk ES; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; **Replace NIDS equipment**

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows

Work in Progress:

Full review of Exchange environment; Exchange baseline monitoring for Tripwire in DRE is ongoing; Purchasing Exchange App for Splunk (contract sent to vendor)

Work Scheduled to Begin Later:

Implement Exchange mail store malware protection

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management

Work in Progress:

Currently investigating Sophos logging functionality

Work not Started:

Finish system planning phase and submit staffing plan and request for funds for email gateway solution; Document O&M requirements for email gateway; Decision on technology for email gateway solution; Complete Sophos replacement project

Work Scheduled to Begin Later:

Investigate WebSense DLP and Email modules; Make decisions on technology for email gateway solution; Replace Sophos equipment;

RT-J-2014-012

Work Scheduled to Begin Later:

Update group policies for Office product macros

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked;

Work in Progress:

Evaluating SPC Admin group rights; Changes to draft updated Windows 7 standard; Improve management of SPC laptops; Currently performing cleanup in IVC DRE (development domain); Clean up Citrix group policies

Work not Started:

Enforce group policy change control policies and procedures

Work Scheduled to Begin Later:

Upgrade WebSense; Implement Web Proxy to replace EoLWebSense

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE

Work in Progress:

Full push of policy in DRE; Implement password policies for EPU and service accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives;"
Implement automated inventory of authorized and unauthorized devices

Work not Started:

Identify staffing plan and implement process for resolution of future logging support.

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising our mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team's objectives were BPA's mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Percentages Complete

The graph below represents the amount of remediation work completed for each POA&M on a particular date.

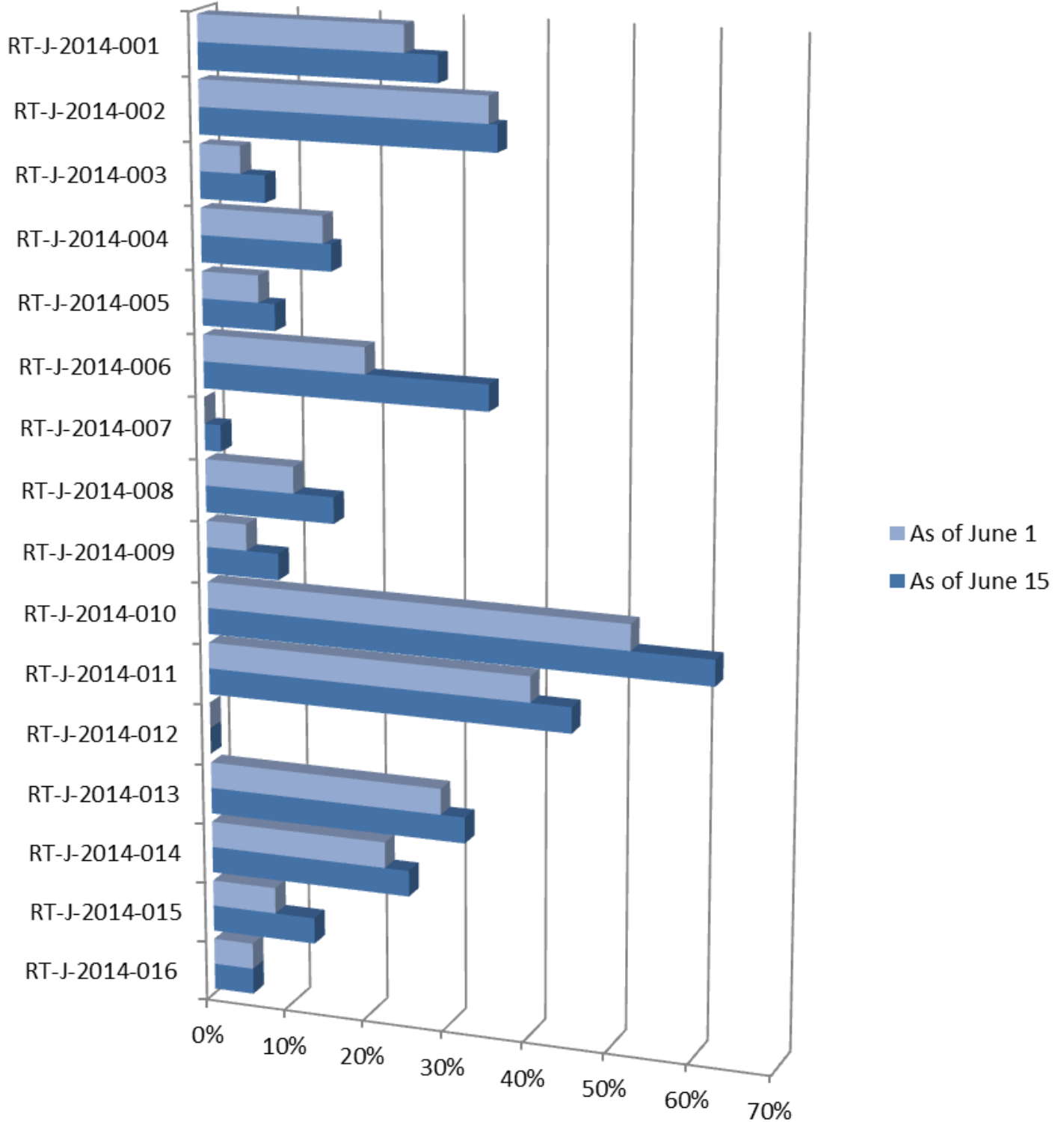
The percentage complete for each activity, represents a point-in-time estimation of work complete. As remediation progresses the need for additional work may become necessary. Thus, the percentages may vary over time.

Each percentage complete is represented by two bars. In order to illustrate the amount of progress made since the last report was issued, the *percent complete* is shown for the previous report as well.

The section appearing below the graph outlines each POAM, and divides tasks into those that are *Complete*, *In Progress*, *Not Started*, and *Scheduled to Begin at a Later Date*.

POA&M Percent Complete

POA&M Number Percentage Complete as of June 15, 2015: *Note, RT-J-2014-016 was re-evaluated and a new strategy is being developed.*



POA&M Details

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M

Remediation Tasks

(some tasks address multiple POA&Ms)

RT-J-2014-001

Work Completed:

Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Remove unused lan.bat legacy settings; Update lan.bat permissions; Drive mapping solution is chosen (staying with lan.bat for primary drive mapping purposes)

Work in Progress:

Remove Unnecessary users from admin groups; Team is reviewing 37 other unique .bat files called within lan.bat; Cleaning up legacy calls.

Work Scheduled to Begin Later:

Choose technologies for FIM solution; Complete list of high risk systems; Develop automated asset inventory to allow monitoring of new systems; Evaluate *File Integrity Monitoring* (FIM) implementation

RT-J-2014-002

Work Completed:

Evaluate implementation of AppLocker temp directory; Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Choose technology for EndPoint Protection Solution; installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work not Started:

Choose technology for temp directory whitelisting

Work Scheduled to Begin Later:

Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; Complete list of high risk systems

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Ensure new NIDS logs are ingested by Splunk; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Renew contract and review support for Cisco *Network Intrusion Detection System* (NIDS); Evaluate implementation of Splunk *Enterprise Security* (ES); installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work not Started:

Requirements gathering for NIDS technology; **Choose NIDS technology; Finish NIDS system planning phase and submit staffing plan and request for funds; Document O&M requirements for NIDS solution; Ensure NIDS logs response procedures are in place;**

RT-J-2014-004**Work Completed:**

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

RT-J-2014-005**Work Completed:**

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Installation of TrendMicro software in DRE for testing; ; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting

RT-J-2014-006**Work Completed:**

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded.

Work in Progress:

Changes to draft updated Windows 7 standard; Upgrade Check Point FWs to most recent version; Cleanup workstation group policies; Cleanup Citrix group policies; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Replace perimeter Check Point FWs; Implement endpoint protection suite incorporating application whitelisting; Upgrade WebSense; Select and implement Web Proxy to replace EoL for WebSense

RT-J-2014-007**Work Complete:**

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk;

Work Scheduled to Begin Later:

Investigate *Data Loss Prevention* (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; **Replace NIDS equipment**; Evaluate implementation of Splunk ES; Implement a Web Application FW;

RT-J-2014-008**Work Completed:**

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Ensure CSOAC receives proper NIDS feeds; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; Core license upgrade received and successfully installed. HQ firewalls are successfully upgraded.

Work in Progress:

Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Upgrade WebSense; Replace EoL WebSense

RT-J-2014-009**Work Complete:**

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Implement Splunk ES; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; **Replace NIDS equipment**

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows

Work in Progress:

Full review of Exchange environment; Exchange baseline monitoring for Tripwire in DRE is ongoing; Purchasing Exchange App for Splunk (contract sent to vendor)

Work Scheduled to Begin Later:

Implement Exchange mail store malware protection

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management

Work in Progress:

Currently investigating Sophos logging functionality

Work not Started:

Finish system planning phase and submit staffing plan and request for funds for email gateway solution; Document O&M requirements for email gateway; Decision on technology for email gateway solution; Complete Sophos replacement project

Work Scheduled to Begin Later:

Investigate WebSense DLP and Email modules; Make decisions on technology for email gateway solution; Replace Sophos equipment;

RT-J-2014-012

Work Scheduled to Begin Later:

Update group policies for Office product macros

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked;

Work in Progress:

Evaluating SPC Admin group rights; Changes to draft updated Windows 7 standard; Improve management of SPC laptops; Currently performing cleanup in IVC DRE (development domain); Clean up Citrix group policies

Work not Started:

Enforce group policy change control policies and procedures

Work Scheduled to Begin Later:

Upgrade WebSense; Implement Web Proxy to replace EoLWebSense

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE

Work in Progress:

Full push of policy in DRE; Implement password policies for EPU and service accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives;"
Implement automated inventory of authorized and unauthorized devices

Work not Started:

Identify staffing plan and implement process for resolution of future logging support.

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete	2
The IT Report	2
The Transmission Report	2
POA&M Percent Complete for IT	3
POA&M Details for IT	4
POA&M Percent Complete for Transmission	10
POA&M Details for Transmission	10
Glossary	13

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The IT Report

For the IT section of the report, each percentage complete is represented by two bars. The current percentage complete can, in this manner, be easily contrasted with the previous reported results.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

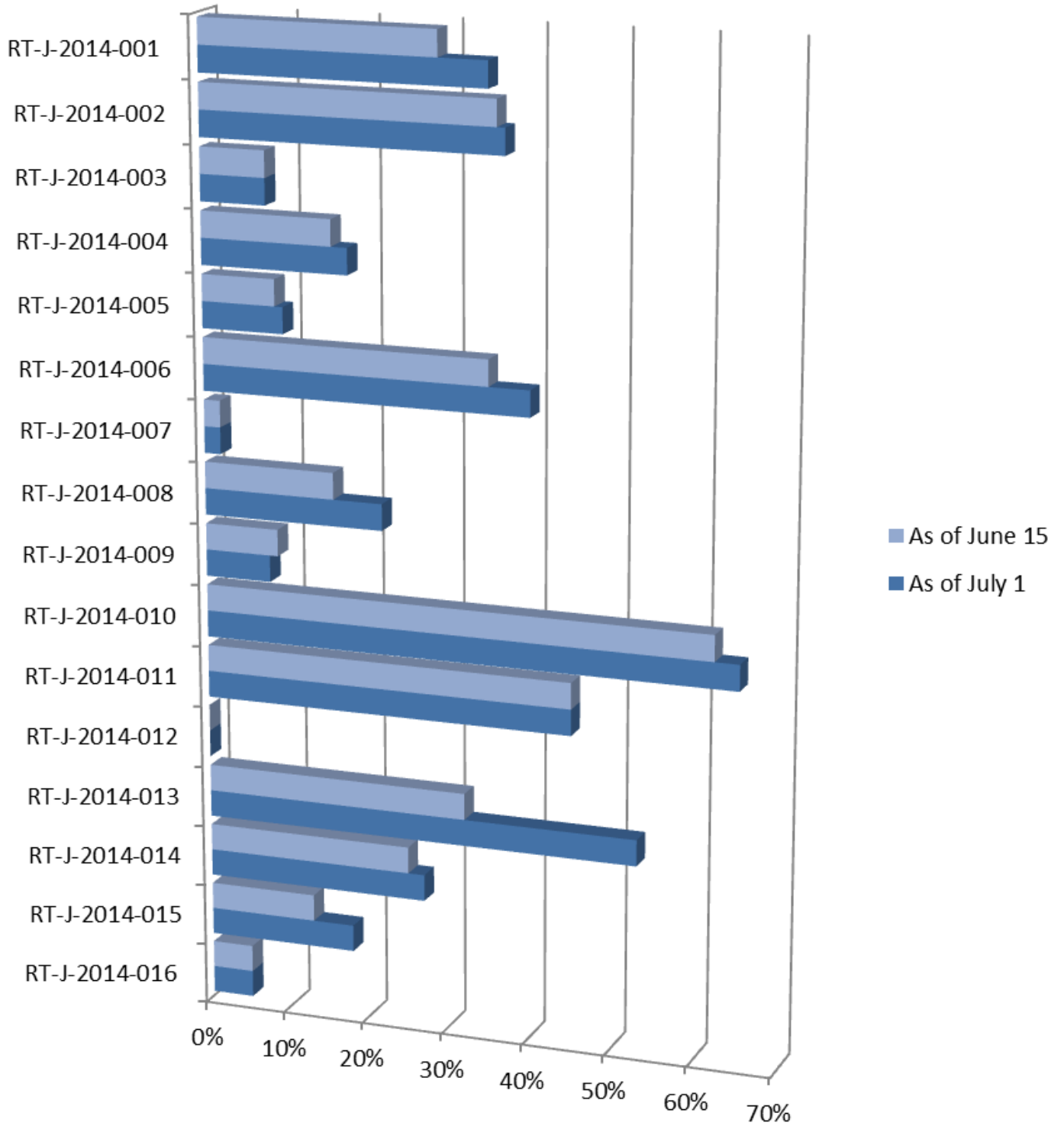
The Transmission Report

This July 1, 2015 report is the first report illustrating the progress of mitigation activities for vulnerabilities that apply to Transmission systems and assets. Therefore, since there were no percentages for Transmission in the previous report, there are no comparisons.

Like the IT Report, the section appearing below the graph for Transmission, outlines each POAM's tasks and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

POA&M Percent Complete for IT

POA&M Number Percentage Complete as of July 1, 2015: *Note, RT-J-2014-016 was re-evaluated and a new strategy is being developed.*



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls</p> <p>Work in Progress: Remove unused lan.bat legacy settings; Remove Unnecessary users from rsc admin groups</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution;</p>	<p>Updated Work in Progress: Deleted legacy member groups; removed desktop admin group; Removed references to legacy .bat files; cleaning up legacy calls</p>
RT-J-2014-002	<p>Work Completed: Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting</p> <p>Work in Progress: Evaluate implementation of AppLocker temp directory; Choose technology for EndPoint Protection Solution; installation of TrendMicro software in DRE for testing; Finish system planning phase for endpoint protection and submit staffing plan and request for funds.</p>	<p>Updated Work in Progress: Testing of Trend Micro for endpoint protection continues; Server components related to Trend Micro application control and HIDS/HIPS have been built</p>

Work Scheduled to Begin Later:

Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; **Complete list of high risk systems**; Rollout endpoint protection solution for servers and workstations

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Evaluate implementation of Splunk Enterprise Security (ES); installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds**; Ensure new NIDS logs are ingested by Splunk

Updated Work in Progress:

Testing of Trend Micro for endpoint protection continues; Server components related to Trend Micro application control and HIDS/HIPS have been built

Work not Started:

Requirements gathering for NIDS technology; Choose NIDS technology; Finish NIDS system planning phase and submit staffing plan and request for funds; Document O&M requirements for NIDS solution; Ensure NIDS logs response procedures are in place;

RT-J-2014-004

Work Completed:

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Updated Work in Progress:

Testing of field engineering debug logging on LDAP events is complete

RT-J-2014-005

Work Completed:

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement FIM including logging; **Implement endpoint protection suite incorporating application whitelisting**

Updated Work in Progress:

Testing of Trend Micro for endpoint protection continues; Server components related to Trend Micro application control and HIDS/HIPS have been built

RT-J-2014-006**Work Completed:**

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

Work in Progress:

Changes to draft updated Windows 7 standard; Cleanup workstation group policies; Cleanup Citrix group policies; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds.**

Work Scheduled to Begin Later:

Implement endpoint protection suite incorporating application whitelisting;
Upgrade WebSense

Updated Work Completed:

The RT-J-2014-webprox and RT-J-2014-web milestones were merged to better reflect the work completed and work in progress for the web proxy architecture at BPA.

Updated Work in Progress:

Testing of Trend Micro for endpoint protection continues; Server components related to Trend Micro application control and HIDS/HIPS have been built; New VDI group policies for Citrix have been promoted to BRE and IRE environments

RT-J-2014-007**Work Complete:**

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk;

Work Scheduled to Begin Later:

Investigate *Data Loss Prevention* (DLP) on Check Point FWs; Implement DLP at the perimeter after UDM project completion and BPA data labeling standard is determined; **Replace NIDS equipment**; Evaluate implementation of Splunk ES; Implement a Web Application FW

RT-J-2014-008

Work Completed:

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs

Work in Progress:

Ensure CSOAC receives proper NIDS feeds; Websense license upgrade received and successfully installed.

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Upgrade WebSense; Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place

Updated Work Complete:

The RT-J-2014-webprox and RT-J-2014-web milestones were merged to better reflect the work completed and work in progress for the web proxy architecture at BPA.

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other

Work in Progress:

Implement Splunk ES; Installation of TrendMicro software in DRE for testing; **Finish system planning phase for endpoint protection and submit staffing plan and request for funds**; **Complete working with CSOAC concerning NIDS feeds in Splunk**

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; **Replace NIDS equipment**; Complete NIDS replacement project; Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place

Updated Work in Progress:

Testing of Trend Micro for endpoint protection continues; Server components related to Trend Micro application control and HIDS/HIPS have been built

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk

Work in Progress:

Exchange baseline monitoring for Tripwire in DRE is ongoing;

Work Scheduled to Begin Later:

Implement Exchange mail store malware protection

Updated Work Complete:

The RT-J-2014-mailgw and RT-J-2014-sophos milestones were merged to better reflect the work completed and work in progress for the mail gateway architecture at BPA. Tripwire tasks for Exchange baseline monitoring in IRE is complete; Splunk Exchange App license was received from GTRI and installed by T Splunk admins

Updated Work in Progress:

COG approved new Exchange Baseline

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management

Work not Started:

Investigate WebSense DLP and Email modules;
Make decisions on technology for email gateway solution

Updated Work Complete:

The RT-J-2014-mailgw and RT-J-2014-sophos milestones were merged to better reflect the work completed and work in progress for the mail gateway architecture at BPA.

RT-J-2014-012

Work Scheduled to Begin Later:

Update group policies for Office product macros

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights;

Updated Work Completed:

The RT-J-2014-webprox and RT-J-2014-web milestones were merged to better reflect the work completed and work in progress for the web proxy architecture at BPA.

Work in Progress:

Changes to draft updated Windows 7 standard; Improve management of SPC laptops; Clean up Citrix group policies; **Enforce group policy change control policies and procedures**; Upgrade WebSense

Updated Work in Progress:

New VDI group policies for Citrix have been promoted to BRE and IRE environments; Cleanup of rscSPCPowerUsers group complete

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE

Work in Progress:

Full push of policy in DRE; Implement password policies for EPU accounts; Cleanup of inactive accounts; Coordinate with CSOAC to reduce false positives for failed login attempts

Updates - Work in Progress:

More inactive accounts were reviewed; more inactive service accounts are ready for deletion; monthly reporting process for inactive accounts has begun

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management; Implement password policies for service accounts

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs

Updated Work Completed:

Concerns around improperly parsed logs are resolved.

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives;" Resolve missing log sources; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; **Identify staffing plan and implement process for resolution of future logging support.**

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

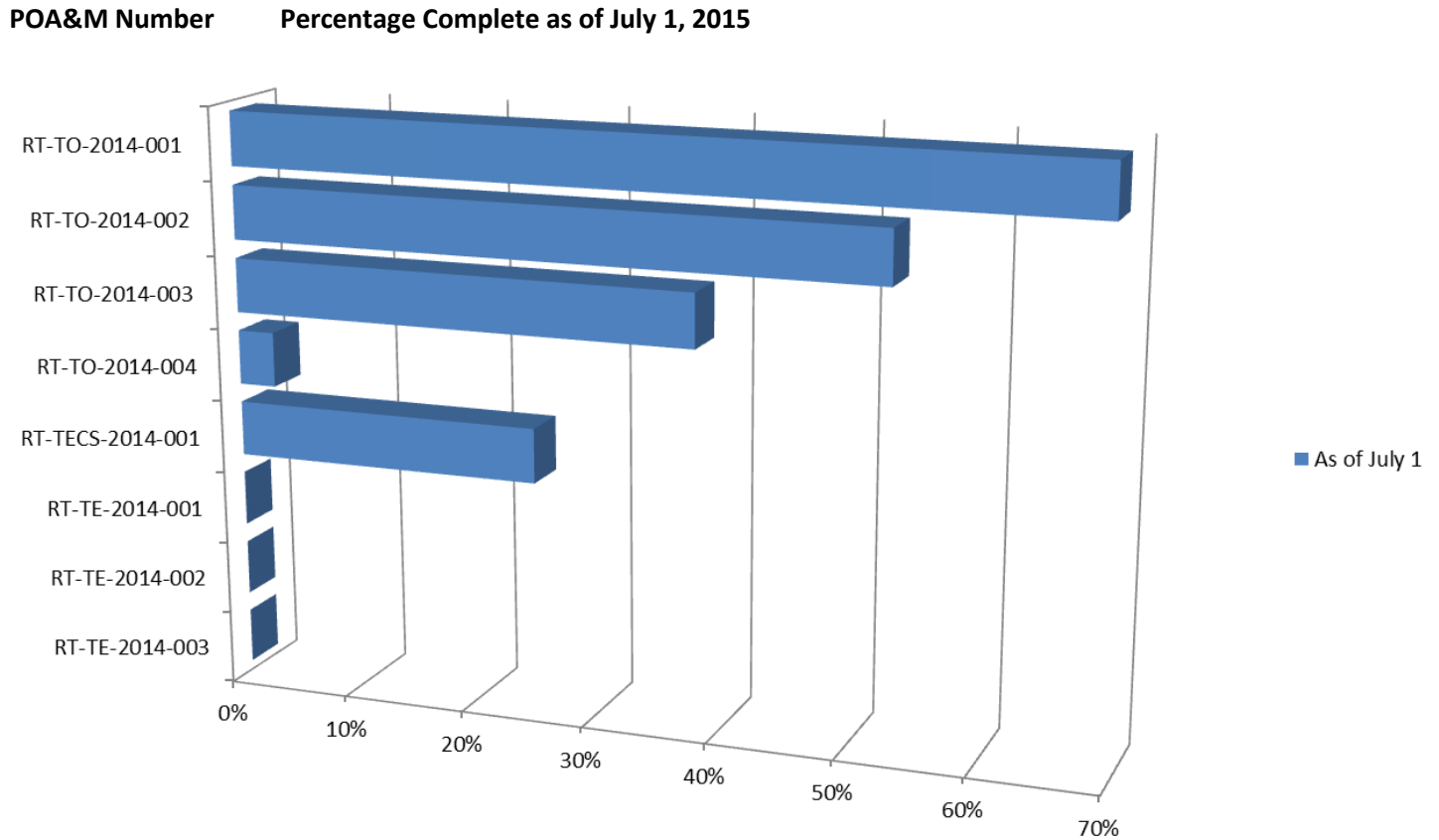
Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

POA&M Percent Complete for Transmission



POA&M Details for Transmission

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M

Remediation Tasks

RT-TO-2014-001

Work Completed:

Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable.

Work in Progress:

Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire.

RT-TO-2014-002**Work Completed:**

Evaluate DGOZ GOPs to ensure only privileged roles can run executable files.

Work in Progress:

Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions.

RT-TO-2014-003**Work Completed:**

Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) *Note: Could only be enforced procedurally*

Work in Progress:

Update Windows Account Management Plan to reflect change in standard;

- 16 character service account passwords
- 12 character interactive user account passwords.

Work not Started:

Create and enforce Control Center issue-specific password policy; Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment.

RT-TO-2014-004**Work in Progress:**

Remove the domain trust from BUD to DGOZ (*Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (*Note: Competing strategies being worked out*)

Work not Started:

Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (*Note: Relying CIP to provide solution*)

RT-TECS-2014-001**Work Completed:**

Purchase and test secure USBs for use on SPC equipment

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens

RT-TE-2014-001

Work not Started:

Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk).

RT-TE-2014-002

Work not Started:

Update the system security (SSP) with authorization boundary and inventory.

RT-TE-2014-003

Work not Started:

Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan.

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Data Loss Prevention** - A system designed to detect potential data breach / data ex-filtration transmissions. DLP solutions monitor, detect and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete.....	2
POA&M Percent Complete for IT.....	3
POA&M Details for IT.....	4
POA&M Percent Complete for Transmission.....	10
POA&M Details for Transmission.....	10
Glossary.....	13

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

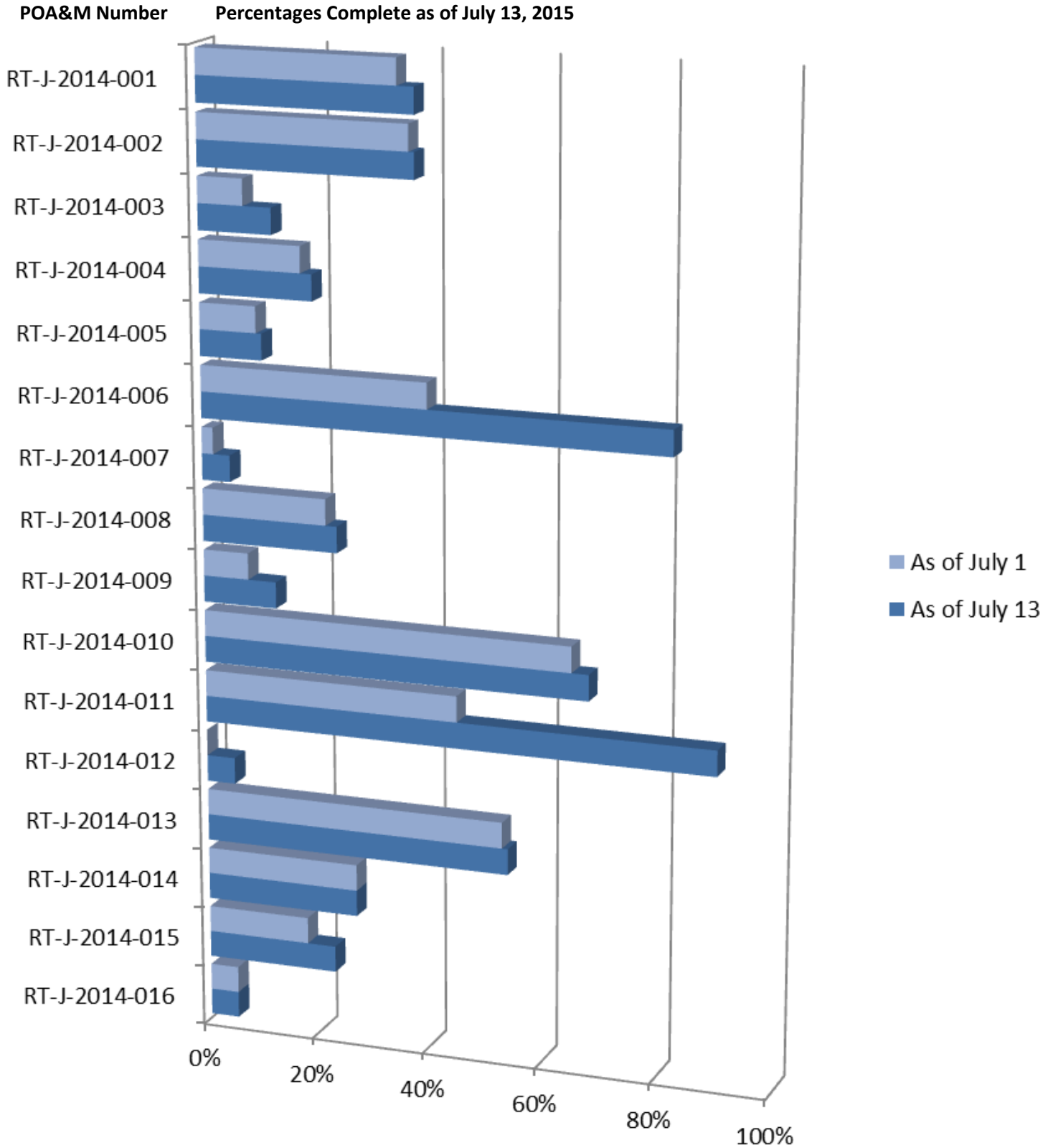
The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

POA&M Percent Complete for IT

RT-J-2014-016 was re-evaluated and a new strategy is being developed.



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls</p> <p>Work in Progress: Remove unused lan.bat legacy settings; Remove Unnecessary users from rsc admin groups</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution</p>	<p>Updated Work in Progress: Documenting procedures for management of lan.bat</p>
RT-J-2014-002	<p>Work Completed: Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory</p> <p>Work in Progress: Choose technology for EndPoint Protection Solution; Finish system planning phase for endpoint protection</p> <p>Work Scheduled to Begin Later: Implementation for logging at endpoints; Complete process for leveraging workstation logs as part of event monitoring; Rollout endpoint protection solution for servers and workstations</p>	<p>Updated Work Completed: Installation of TrendMicro software in DRE for testing</p> <p>Updated Work in Progress: Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec Servers being built; Meeting with Symantec Engineers to finalize module install requirements</p>

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology; Evaluate implementation of Splunk *Enterprise Security* (ES); Finish system planning phase for endpoint protection; Ensure new NIDS logs are ingested by Splunk

Work not Started:

Finish NIDS system planning phase; Document O&M requirements for NIDS solution; Ensure NIDS logs response procedures are in place

Updated Work Completed:

Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS

Updated Work in Progress:

Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec Servers being built; Meeting with Symantec Engineers to finalize module install requirements

RT-J-2014-004

Work Completed:

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased

Work in Progress:

Build Domain Services OU; Domain admins transition to using new management servers; Configure domain controllers to log LDAP events to Splunk; Finish system planning phase for endpoint protection

Updated Work Completed:

LDAP logging implemented on remaining domain controllers in DRE

Updated Work in Progress:

Reviewing performance implications of LDAP logging

RT-J-2014-005

Work Completed:

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing

Work in Progress:

Finish system planning phase for endpoint protection

Updated Work Completed:

Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Updated Work in Progress:

Symantec Servers being built; Meeting with Symantec Engineers to finalize module install requirements

Work Scheduled to Begin Later:

Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting

RT-J-2014-006

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing

Work in Progress:

Changes to draft updated Windows 7 standard; Cleanup workstation group policies; **Cleanup Citrix group policies; Finish system planning phase for endpoint protection; Upgrade WebSense**

Work Scheduled to Begin Later:

Implement endpoint protection suite incorporating application whitelisting

Updated Work Completed:

Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated; Completed testing of Trend Micro for endpoint protection, including Application Control

Updated Work in Progress:

Symantec Servers being built; Meeting with Symantec Engineers to finalize module install requirements; New VDI group policies for Citrix have been promoted to BRE and IRE environments; Purchase request for new WebSense replacement hardware was submitted

RT-J-2014-007

Work Complete:

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk

Work in Progress:

Make a decision on NIDS technology

Work Scheduled to Begin Later:

Replace NIDS equipment; Evaluate implementation of Splunk ES; Implement a Web Application FW

Updated Work Complete:

IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS

RT-J-2014-008

Work Completed:

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Websense license upgrade received and successfully installed

Work in Progress:

Ensure CSOAC receives proper NIDS feeds; Upgrade WebSense

Work Scheduled to Begin Later:

Replace NIDS equipment; Implement Splunk ES; Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place

Updated Work Complete:

IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS

Updated Work in Progress:

Purchase request for new WebSense replacement hardware was submitted

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDS feeds in Splunk

Work in Progress:

Implement Splunk ES; Finish system planning phase for endpoint protection

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting; Replace NIDS equipment; Complete NIDS replacement project; Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place

Updated Work Completed:

Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control

Updated Work in Progress:

Symantec Servers being built; Meeting with Symantec Engineers to finalize module install requirements

RT-J-2014-010**Work Complete:**

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments

Updated Work Complete:

Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

Updated Work in Progress:

Process to create waivers in Tripwire for approved deviations started

RT-J-2014-011**Work Complete:**

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JN1 is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management

Updated Work Complete:

Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR

RT-J-2014-012**Work in Progress:**

Update group policies for Office product macros

Updated Work Completed:

Finished analyzing difference between current MS Office Policies and latest DISA STIG macro settings

RT-J-2014-013**Work Completed:**

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights

Updated Work Completed:

Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated

Work in Progress:

Changes to draft updated Windows 7 standard; Improve management of SPC laptops; **Clean up Citrix group policies; Enforce group policy change control policies and procedures;** Upgrade WebSense

Updated Work in Progress:

Phase 1 testing of SPC laptops has begun; Purchase request for new WebSense replacement hardware was submitted

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE

Work in Progress:

Full push of policy in DRE; Implement password policies for EPU accounts; Cleanup of inactive accounts; **Coordinate with CSOAC to reduce false positives for failed login attempts**

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts; Publish account maintenance guidelines to BITA; Select automated tool for account management; Implement password policies for service accounts

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices

Updated Work Completed:

Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices

Work in Progress:

Work with CSOAC to reduce “failed login” attempts “false positives;” Resolve missing log sources; implement process for resolution of future logging support; Complete list of high risk systems; Resolve high frequency event tuning

Work Scheduled to Begin Later:

Selection of automated asset inventory tool

RT-J-2014-016

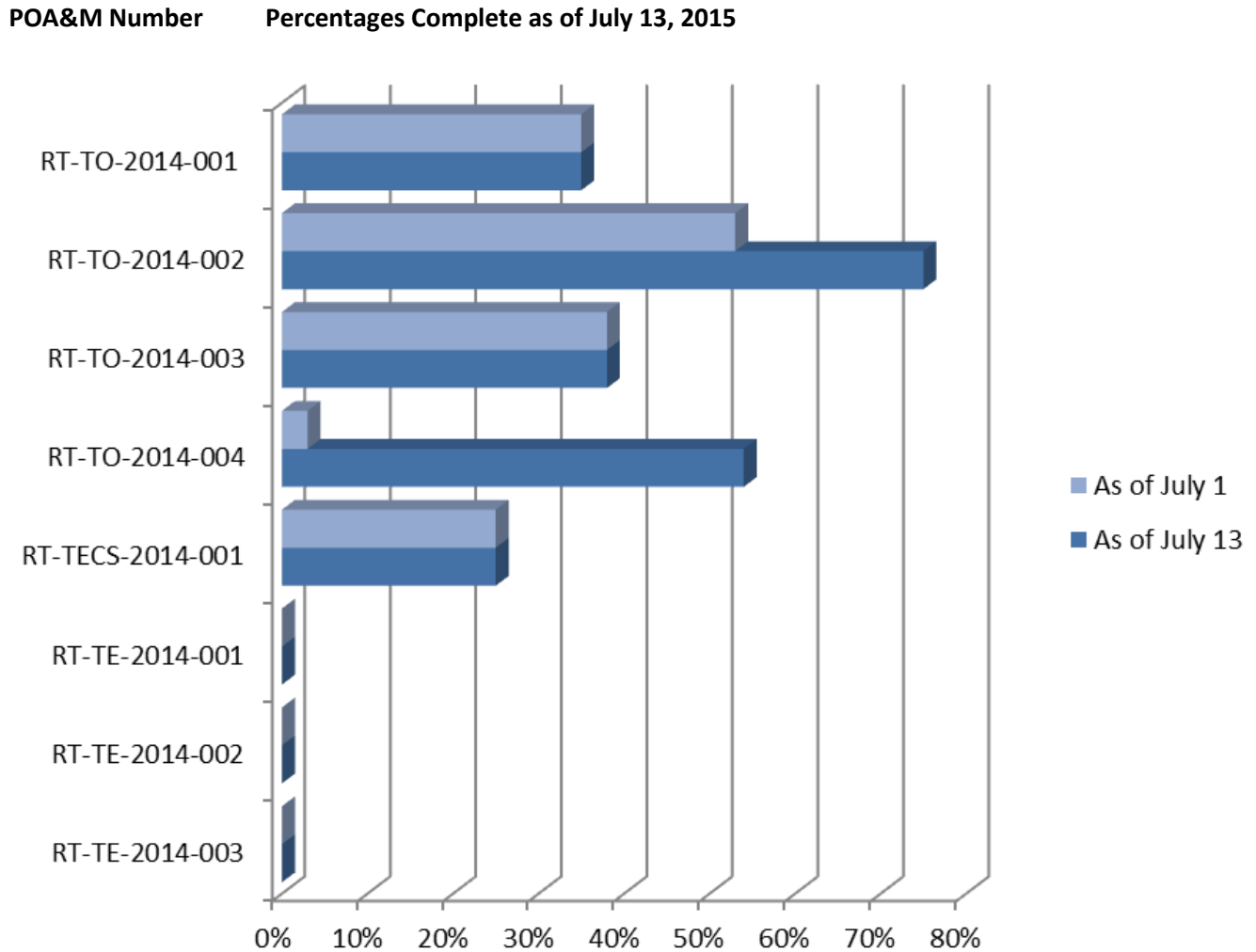
Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

POA&M Percent Complete for Transmission



POA&M Details for Transmission

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M

Remediation Tasks

Progress Updates (tasks updated since last report)

RT-TO-2014-001

Work Completed:
 Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs

where capable.

Work in Progress:

Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire

RT-TO-2014-002

Work Completed:

Evaluate DGOZ GOPs to ensure only privileged roles can run executable files

Work in Progress:

Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions

Updated Work in Progress:

The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution

RT-TO-2014-003

Work Completed:

Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) *Note: Could only be enforced procedurally*

Work in Progress:

Update Windows Account Management Plan to reflect change in standard;

- 16 character service account passwords
- 12 character interactive user account passwords

Work not Started:

Create and enforce Control Center issue-specific password policy; Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment

RT-TO-2014-004

Work in Progress:

Remove the domain trust from BUD to DGOZ (*Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (*Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (*Note: Relying CIP to provide solution*)

Updated Work in Progress:

Progress was made on resolving competing strategies between the Control Center and Corporate IT; Progress was made on reviewing the necessity of all ports and services transgressing the DMZ boundary

- RT-TECS-2014-001** **Work Completed:**
Purchase and test secure USBs for use on SPC equipment
- Work not Started:**
Enable security on all FIN connected GE D-400s;
Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens
- RT-TE-2014-001** **Work not Started:**
Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk)
- RT-TE-2014-002** **Work not Started:**
Update the system security (SSP) with authorization boundary and inventory
- RT-TE-2014-003** **Work not Started:**
Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete	2
POA&M Percent Complete for IT	3
POA&M Details for IT	4
POA&M Percent Complete for Transmission	15
POA&M Details for Transmission	16
Glossary	18

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

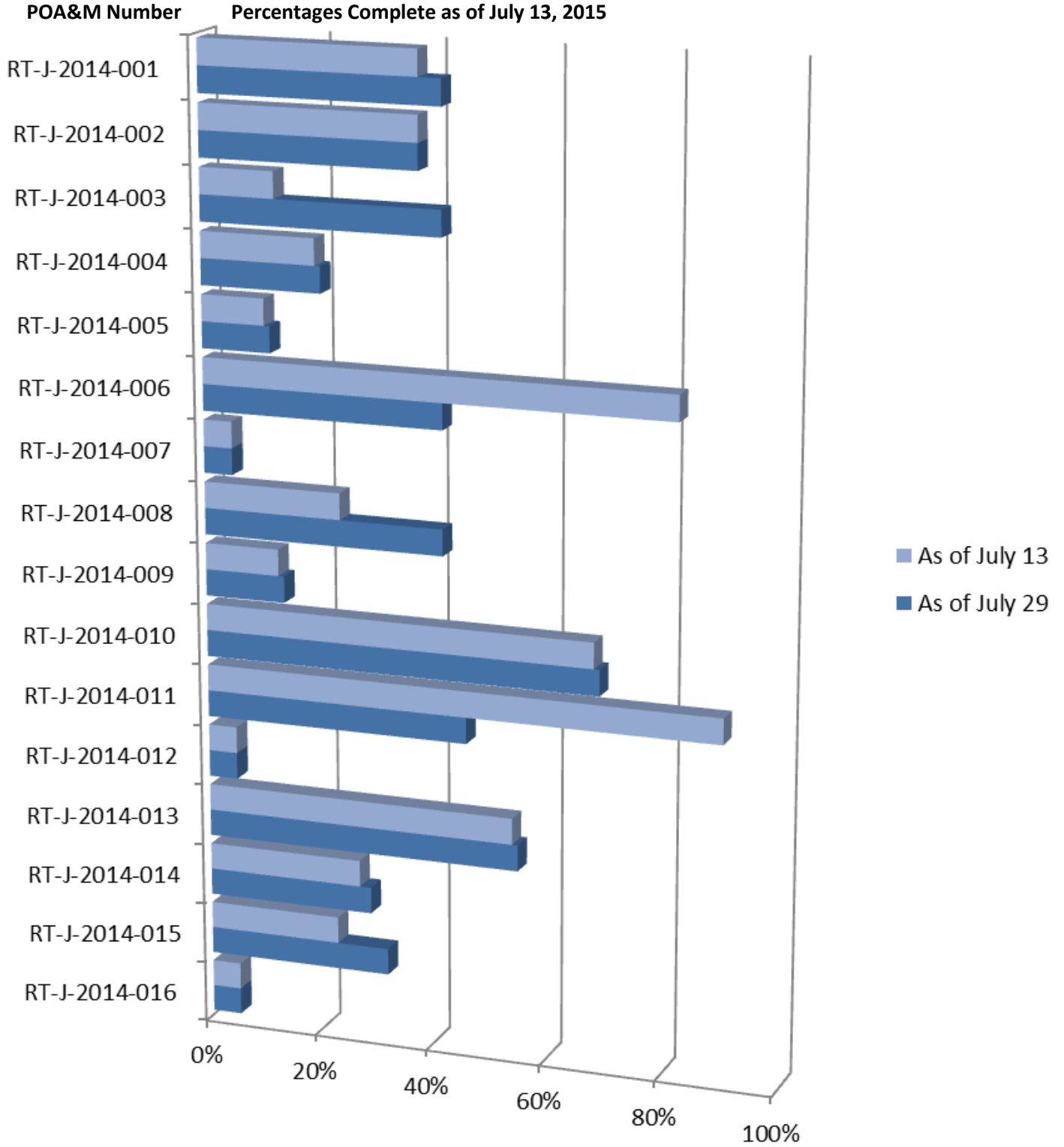
The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

POA&M Percent Complete for IT

RT-J-2014-016 was re-evaluated and a new strategy is being developed.



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)	Team
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat</p> <p>Work in Progress: Ongoing efforts to remove unnecessary member groups (completion due- 7/31/2015)</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution (completion due- 6/26/2015)</p>	<p>Updated Work Completed: Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat</p>	Betty Pedersen, Steve Ireland

RT-J-2014-002

Work Completed:

Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Choose technology for EndPoint Protection Solution; Finish system planning phase for endpoint protection (completion due-3/30/2015)

Work Scheduled to Begin Later:

Implementation for logging at endpoints (10/23/2015); Complete process for leveraging workstation logs as part of event monitoring (10/30/2015); Rollout endpoint protection solution for servers and workstations (10/30/2015)

Updated Work in Progress:

Symantec Servers being built; Symantec proof of concept in process

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(logging at endpoints)
Chris Glanville

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing; Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology (no date); Evaluate implementation of Splunk Enterprise Security (ES); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Ensure new NIDS logs are ingested by Splunk (no date)

Work not Started:

Finish NIDS system planning phase (no date); Document O&M requirements for NIDS solution(no date); Ensure NIDS logs response procedures are in place (no date)

Updated Work in Progress:

Symantec proof of concept in process; Cisco FireSight PO being leveraged

(endpoint protection) Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans (NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (Splunk) Ross Bradley, Chris Glanville

RT-J-2014-004

Work Completed:

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased; LDAP logging implemented on domain controllers in DRE

Updated Work Completed:

Performance review of domain controllers running LDAP logging is complete with no significant impact

(LDAP event logging on all domain controllers)Chris Glanville, Betty Pedersen, John O'Donnell

Work in Progress:

Build Domain Services OU
(completion due – 6/30/2015);
Domain admins transition to using
new management
servers(completion due –
6/30/2015); Configure domain
controllers to log LDAP events to
Splunk(completion due –
6/30/2015)

RT-J-2014-005

Work Completed:

Requirements gathering for
endpoint protection; Firewall
changes made in DRE to allow
testing of Trend Micro servers
communications with each
other; Installation of TrendMicro
software in DRE for testing;
Completed testing of Trend Micro
for endpoint protection, including
Application Control

Work in Progress:

Finish system planning phase for
endpoint protection (completion
due- 3/30/2015)

Updated Work in Progress:

Symantec proof of concept in
process

Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans

Work Scheduled to Begin Later:

Implement FIM including logging;
Implement endpoint protection
suite incorporating application
whitelisting (6/26/2015)

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated; Completed testing of Trend Micro for endpoint protection, including Application Control ; New VDI group policies for Citrix have been promoted to BRE and IRE environments; Purchase request for new WebSense replacement hardware was submitted

Work in Progress:

Changes to draft updated Windows 7 standard (12/4/2015); Cleanup workstation group policies (12/4/2015); **Cleanup Citrix group policies (7/15/2015); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Upgrade WebSense (8/14/2015)**

Updated Work Completed:

The WebProxy group of tasks was removed from this POAM and merged with the Web group of tasks in POAM 013 (the removal of this group of tasks, resulted in an adjustment of progress complete to a lesser percentage); A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Updated Work in Progress:

Symantec proof of concept in process; Scans revealed 94% compliance with Win 7 policies; Deviations from policies are being documented

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
Katie Feucht; (Websense)
Jason Enger; (Citrix) Eric
Wilson, Katie Feucht

Work Scheduled to Begin Later:
Implement endpoint protection suite incorporating application whitelisting (3/30/2015)

RT-J-2014-007

Work Complete:
Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk

Work in Progress:
Make a decision on NIDS technology (no date)

Work Scheduled to Begin Later:
Replace NIDS equipment (no date); Evaluate implementation of Splunk ES; Implement a Web Application FW (10/2/2015)

Updated Work Complete:
IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS

Updated Work in Progress:
Cisco FireSight PO being leveraged

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (web application FW) Chuck Dockery, Jason Enger

RT-J-2014-008

Work Completed:
Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Websense license upgrade received and successfully installed; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS

Work in Progress:
Ensure CSOAC receives proper NIDS feeds (no date); Upgrade WebSense (8/14/2015)

Updated Work Completed:
The WebProxy group of tasks was removed from this POAM and merged with the Web group of tasks in POAM 013; A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Updated Work in Progress:
Cisco FireSight PO being leveraged

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (Websense) Jason Enger

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Implement Splunk ES; Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDs feeds in Splunk; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Implement Splunk ES; Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting (3/30/2015); Replace NIDS equipment (no date); Complete NIDs replacement project (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

Updated Work in Progress:

Symantec proof of concept in process; Cisco FireSight PO being leveraged

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen

RT-J-2014-010**Work Complete:**

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments; Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

Updated Work in Progress:
Negotiating with Cyber re: Exchange Teams process for updating Sophos rules (no date)

Darlene Williams, Betty Pedersen

RT-J-2014-011**Work Complete:**

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JN1 is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management; Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR

Updated Work Complete:

The MailGW group of tasks was removed from this POAM and merged with the Sophos group of tasks in POAM 010 (the removal of this group of tasks, resulted in an adjustment of progress complete to a lesser percentage)

Updated Work in Progress:
Negotiating with Cyber re:
Exchange Teams process for
updating Sophos rules (no
date)

Darlene Williams, Betty
Pedersen

RT-J-2014-012

Updated Work Completed:
Finished analyzing difference
between current MS Office
Policies and latest DISA STIG
macro settings

Loyd Towe, Matt Buss,
Katie Feucht

Work in Progress:
Update group policies for Office
product macros (12/30/2015)

RT-J-2014-013

Work Completed:
Local Admin accounts have been
moved to a new OU structure,
including WebSense blocking
Internet access; Configure WCCP
to force web traffic from myPC
network through WebSense;
Tighten group policy change
control procedures; Changes to
draft updated Windows 7 USGCB
baseline; Test workstation
created; New SPC OU structure in
Bud finished with new SPC group
policy linked; Evaluating SPC
Admin group rights; Power
settings have been reviewed and
updated

Updated Work Completed:
Ken Ballou finished with first
round of testing; A contract has
been awarded to Assurance
Data for Websense appliances
relevant to the Websense
upgrade.

Work in Progress:
Changes to draft updated
Windows 7 standard
(12/15/2015); **Improve
management of SPC laptops (no
date); Clean up Citrix group
policies (7/15/2015); Enforce
group policy change control
policies and procedures
(4/24/2015); Upgrade WebSense
(8/14/2015)**

Updated Work in Progress:
Scans revealed 94% compliance
with Win 7 policies; Deviations
from policies are being
documented; Planning next
phase of testing with SPC users
to resolve legacy IE and host
firewall issues

(Win 7 Policies) Aurther
Bendetti-White, Loyd
Towe, Pete Albert, Chris
Glanville, Earl Evans; Katie
Feucht; (Websense) Jason
Enger; (SPC laptops) Loyd
Towe, Ken Ballou); (group
policies) Betty Pedersen

RT-J-2014-014**Work Complete:**

Update weak passwords; Phase 1 testing in DRE; 12 inactive standard accounts were disabled and scheduled for deletion; Inactive account script updated to better sanitize out of scope accounts

Work in Progress:

Full push of policy in DRE (5/29/2015); Implement password policies for EPU accounts (5/29/2015); Cleanup of inactive accounts (8/15/2015); Coordinate with CSOAC to reduce false positives for failed login attempts (5/1/2015); Implement password policies for service accounts (12/30/2015)

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts (9/30/2015); Publish account maintenance guidelines to BITA; Select automated tool for account management

Updated Work in Progress:

15 character password enforced for 120 EPU users in DRE

(inactive accounts) Betty Pedersen, Steve Ireland; (failed login attempts) Chris Clanville, David, Mullin, Brian Dugan

RT-J-2014-015**Work Completed:**

Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; implement process for resolution of future logging support

Updated Work Completed:

CSOAC confirmed VmWare VCenter and Mail Header logs are being sent to Splunk (from finalized list of missing log sources); Fixed svcNOC-WMIAdmin and epuSOMag (from finalized list of top accounts with excessive failed logons)

(logging) Chris Clanville, David, Mullin, Brian Dugan

Work in Progress:

Work with CSOAC to reduce
“failed login” attempts “false
positives” (5/1/2015); Resolve
missing log sources (6/16/2015);
Resolve high frequency event
tuning (6/19/2015)

Work Scheduled to Begin Later:

Selection of automated asset
inventory tool (no date)

RT-J-2014-016

Work in Progress (but on hold):

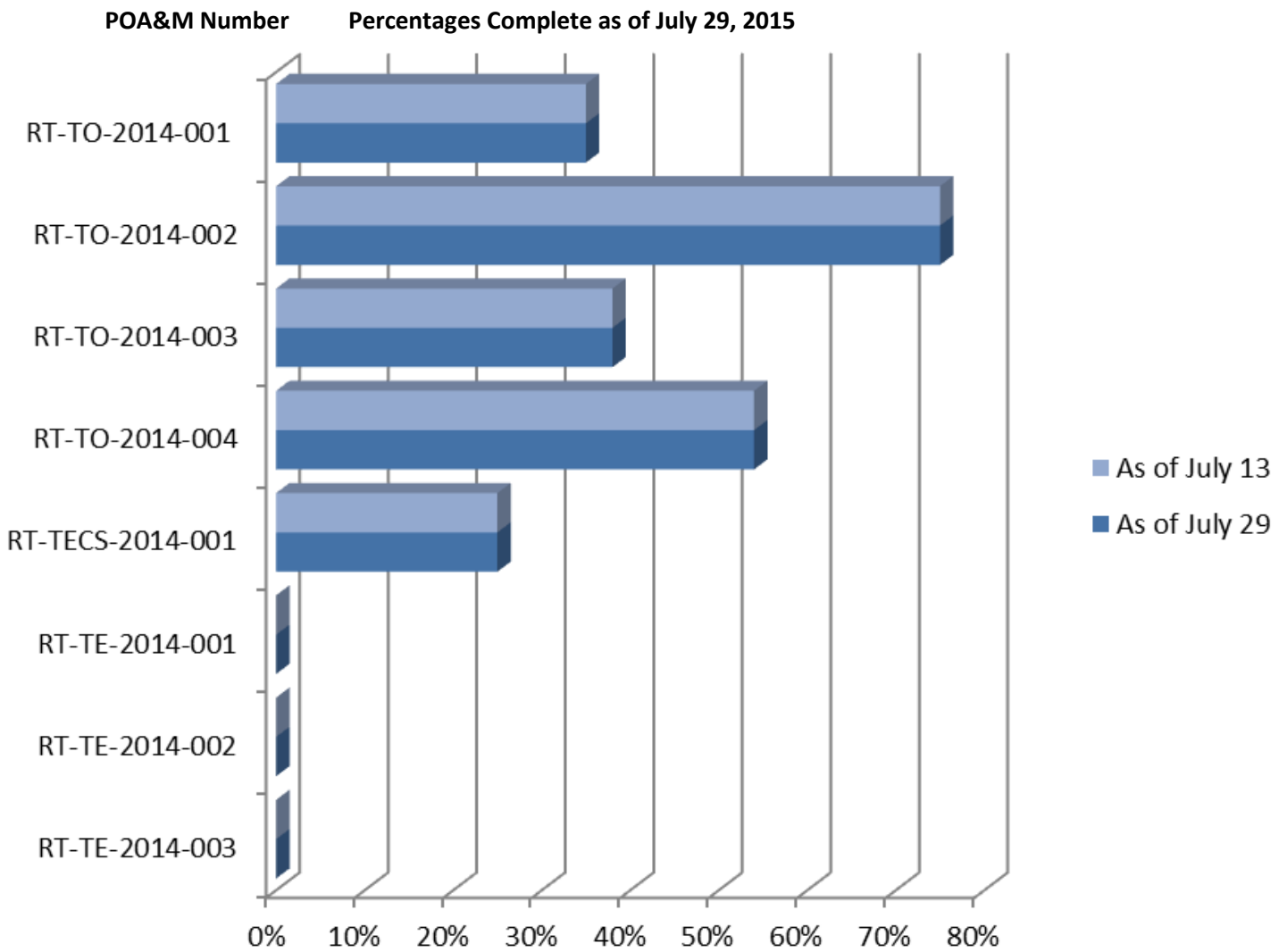
Evaluate and document domain
trusts and FW rules between
various environments

Work Scheduled to Begin Later:

Evaluate and document domain
trusts and FW rules between Grid
Ops and IT Ops; Implement new
FW rule configurations

POA&M Percent Complete for Transmission

(no change in progress since the last report)



POA&M Details for Transmission

(no change in progress since the last report)

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M

Remediation Tasks

Progress Updates

(no progress since last report)

RT-TO-2014-001

(Tim Eubanks)

Work Completed:

Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable.

Work in Progress:

Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire

RT-TO-2014-002

(Tim Eubanks)

Work Completed:

Evaluate DGOZ GOPs to ensure only privileged roles can run executable files; The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution

Work in Progress:

Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions

RT-TO-2014-003

(Tim Eubanks)

Work Completed:

Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) *Note: Could only be enforced procedurally*

Work in Progress:

Update Windows Account Management Plan to reflect change in standard;

- 16 character service account passwords
- 12 character interactive user account passwords

Work not Started:

Create and enforce Control Center issue-specific password policy; Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment

RT-TO-2014-004

(Tim Eubanks)

Work in Progress:

Remove the domain trust from BUD to DGOZ (*Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (*Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (*Note: Relying CIP to provide solution*); Progress was made on resolving competing strategies between the Control Center and Corporate IT; Progress was made on reviewing the necessity of all ports and services transgressing the DMZ boundary

RT-TECS-2014-001

(Scott Lissit)

Work Completed:

Purchase and test secure USBs for use on SPC equipment

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens

RT-TE-2014-001

(unknown)

Work not Started:

Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk)

RT-TE-2014-002

(unknown)

Work not Started:

Update the system security (SSP) with authorization boundary and inventory

RT-TE-2014-003
(unknown)

Work not Started:

Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.

- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms), and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete.....	2
POA&M Percent Complete for IT.....	3
POA&M Details for IT.....	4
POA&M Percent Complete for Transmission.....	15
POA&M Details for Transmission.....	16
Glossary.....	18

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

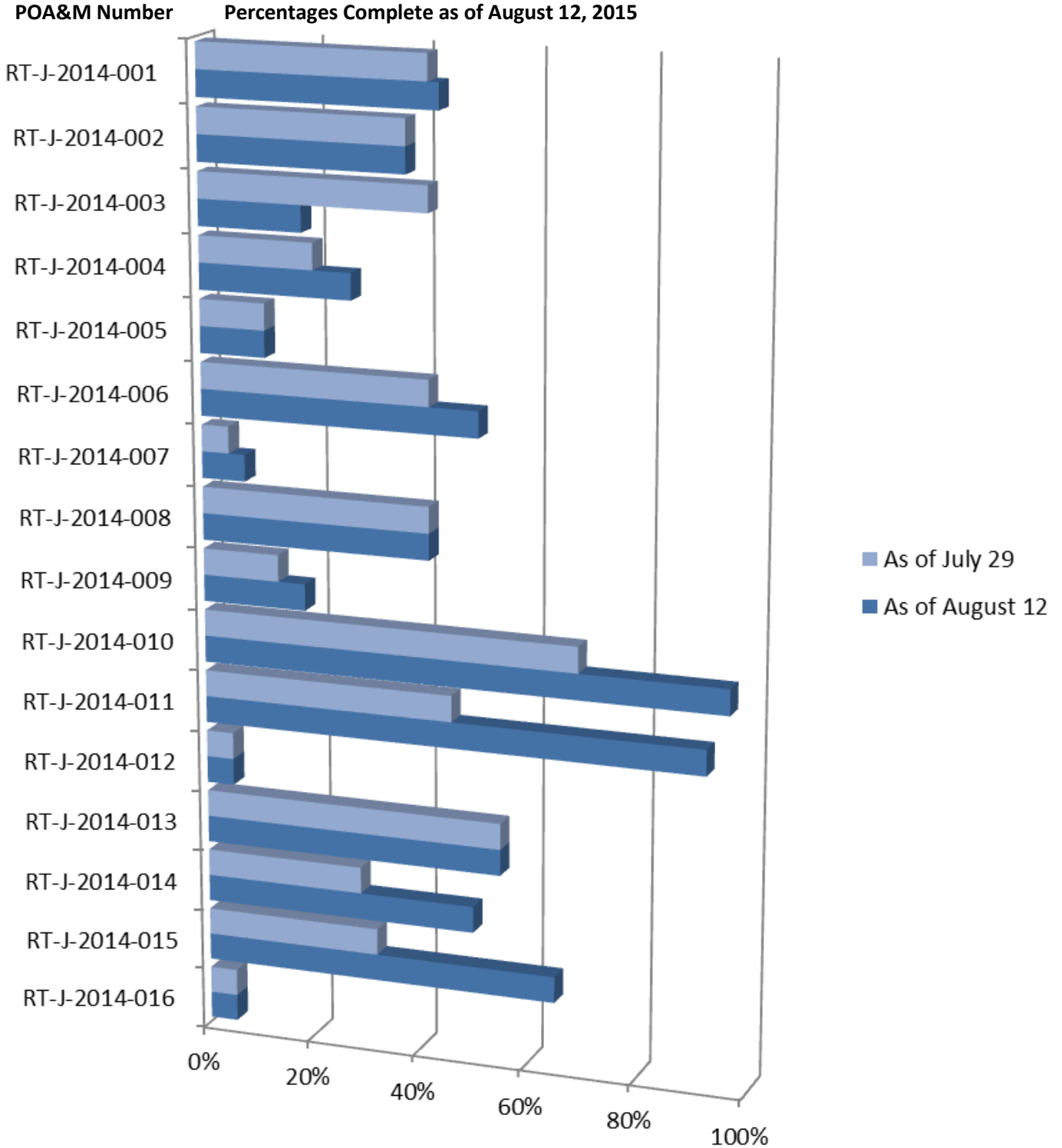
The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

Mitigation activities across all teams, IT and Transmission, are 37% complete

POA&M Percent Complete for IT

Mitigation activities for J, across all POA&Ms, are 39% complete

RT-J-2014-016 was re-evaluated and a new strategy is being developed.



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)	Team
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat (8/7/2015)</p> <p>Work in Progress: Ongoing efforts to remove unnecessary member groups (completion due- 7/31/2015)</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution (completion due- 6/26/2015)</p>	<p>Updated Work Completed: Confirmed that all tasks are complete for lan.bat cleanup and implementation of automated creation (8/7/2015)</p>	Betty Pedersen, Steve Ireland

RT-J-2014-002

Work Completed:

Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(logging at endpoints)
Chris Glanville

Work in Progress:

Choose technology for EndPoint Protection Solution; Finish system planning phase for endpoint protection (completion due-3/30/2015);

Work Scheduled to Begin Later:

Implementation for logging at endpoints (10/23/2015); Complete process for leveraging workstation logs as part of event monitoring (10/30/2015); Rollout endpoint protection solution for servers and workstations (10/30/2015)

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing; Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS;

Note: Several Splunk ES related tasks formerly accepted as addressing this POA&M, relate more directly to the Transmission group, and are no longer being tracked with J's mitigation efforts.

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (Splunk)
Ross Bradley, Chris
Glanville

Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec proof of concept; Cisco FireSight PO leveraged

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology (no date); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Ensure new NIDS logs are ingested by Splunk (no date)

Work not Started:

Finish NIDS system planning phase (no date); Document O&M requirements for NIDS solution(no date); Ensure NIDS logs response procedures are in place (no date)

Updated Work in Progress:

Cisco Firesight appliances have been received

RT-J-2014-004

Work Completed:

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased; LDAP logging implemented on domain controllers in DRE

Work in Progress:

Build Domain Services OU (completion due – 6/30/2015); Domain admins transition to using new management servers(completion due – 6/30/2015); Configure domain controllers to log LDAP events to Splunk (completion due – 6/30/2015)

Updated Work Completed:

LDAP logging successfully implemented in BRE and IRE

(LDAP event logging on all domain controllers)Chris Glanville, Betty Pedersen, John O'Donnell

RT-J-2014-005

Work Completed:

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement FIM including logging;
Implement endpoint protection suite incorporating application whitelisting (6/26/2015)

RT-J-2014-006

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on firewalls (FWs); Configure Web Cache Communications Protocol (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have

Updated Work Completed:

Recommended workstation group policies baseline is complete

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
Katie Feucht; (Websense)
Jason Enger; (Citrix) Eric
Wilson, Katie Feucht

been reviewed and updated;
Completed testing of Trend Micro
for endpoint protection, including
Application Control ; New VDI
group policies for Citrix have been
promoted to BRE and IRE
environments; Purchase request
for new WebSense replacement
hardware was submitted

Work in Progress:

Changes to draft updated
Windows 7 standard (12/4/2015);
Cleanup workstation group
policies (12/4/2015); **Cleanup
Citrix group policies (7/15/2015);
Finish system planning phase for
endpoint protection (completion
due- 3/30/2015); Upgrade
WebSense (8/14/2015)**

Updated Work in Progress:

Websense appliances are being
inventoried

Work Scheduled to Begin Later:

**Implement endpoint protection
suite incorporating application
whitelisting (3/30/2015)**

RT-J-2014-007

Work Complete:

Review Cisco support contract for
NIDS, ensuring receipt of new
signatures; Ensure CSOAC is
receiving NIDS feeds; Resolve
versioning conflict between NIDS
and Splunk

(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (web
application FW) Chuck
Dockery, Jason Enger

Work in Progress:

**Make a decision on NIDS
technology (no date)**

Updated Work in Progress:

Cisco FireSight PO being
leveraged

Work Scheduled to Begin Later:

**Replace NIDS equipment (no
date); Evaluate implementation of
Splunk ES; Implement a Web
Application FW (10/2/2015)**

RT-J-2014-008

Work Completed:

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Websense license upgrade received and successfully installed; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Work in Progress:

Ensure CSOAC receives proper NIDS feeds (no date); Upgrade WebSense (8/14/2015)

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Implement Splunk ES; Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

Note: Several Splunk ES related tasks formerly accepted as addressing this POA&M, relate more directly to the Transmission group, and are no longer being tracked with J's mitigation efforts.

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (Websense) Jason Enger

Updated Work in Progress:

Cisco FireSight PO being leveraged

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDS feeds in Splunk; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Implement Splunk ES; Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting (3/30/2015); Replace NIDS equipment (no date); Complete NIDS replacement project (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

Note: Several Splunk ES related tasks formerly accepted as addressing this POA&M, relate more directly to the Transmission group, and are no longer being tracked with J's mitigation efforts.

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen

Updated Work in Progress:

Cisco FireSight PO being leveraged

RT-J-2014-010**Work Complete:**

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments; Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

Updated Work Complete:

Exchange / mail environment review is complete

Note: The exchav group of milestone tasks was removed from this POAM, since the issue of Exchange mail storage protection is included in the exch group of milestone tasks. The removal of this group of tasks moved the percentage complete forward.

Darlene Williams, Betty Pedersen

Updated Work in Progress:

Process for updating Sophos rules may now be complete (no date)

RT-J-2014-011**Work Complete:**

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management; Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR

Note:

The DLP group of tasks was removed from this POA&M since DLP does not directly address the vulnerabilities described. The percentage complete advanced.

Darlene Williams, Betty Pedersen

RT-J-2014-012**Updated Work Completed:**

Finished analyzing difference between current MS Office Policies and latest DISA STIG macro settings

Loyd Towe, Matt Buss,
Katie Feucht

Work in Progress:

Update group policies for Office product macros (12/30/2015)

RT-J-2014-013**Work Completed:**

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights; Power settings have been reviewed and updated

Updated Work Completed:

Recommended workstation group policies baseline is complete

Work in Progress:

Changes to draft updated Windows 7 standard (12/15/2015); **Improve management of SPC laptops (no date); Clean up Citrix group policies (7/15/2015); Enforce group policy change control policies and procedures (4/24/2015); Upgrade WebSense (8/14/2015)**

(Win 7 Policies) Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans; Katie Feucht; (Websense) Jason Enger; (SPC laptops) Loyd Towe, Ken Ballou); (group policies) Betty Pedersen

RT-J-2014-014**Work Complete:**

Update weak passwords; Phase 1 testing in DRE; 12 inactive standard accounts were disabled and scheduled for deletion; Inactive account script updated to better sanitize out of scope accounts

Work in Progress:

Full push of policy in DRE (5/29/2015); Implement password policies for EPU accounts (5/29/2015); Cleanup of inactive accounts (8/15/2015); Coordinate with CSOAC to reduce false positives for failed login attempts (5/1/2015); Implement password policies for service accounts (12/30/2015)

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts (9/30/2015); Publish account maintenance guidelines to BITA; Select automated tool for account management

Updated Work Complete:

Draft documented process is created; EPU accounts are fully applied in DRE; Password script implementation finalized

Updated Work in Progress:

Continued disabling inactive accounts; Review of inactive service accounts is ongoing

(inactive accounts) Betty Pedersen, Steve Ireland; (failed login attempts) Chris Clanville, David, Mullin, Brian Dugan

RT-J-2014-015**Work Completed:**

Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; implement process for resolution of future logging support

Note: The inv group of tasks was removed from this POAM since they did not directly address the vulnerabilities identified. Therefore, the percentage complete advanced.

(logging) Chris Clanville, David, Mullin, Brian Dugan

Work in Progress:

Work with CSOAC to reduce
“failed login” attempts “false
positives” (5/1/2015); Resolve
missing log sources (6/16/2015);
Resolve high frequency event
tuning (6/19/2015)

Work Scheduled to Begin Later:

Selection of automated asset
inventory tool (no date)

RT-J-2014-016

Work in Progress (but on hold):

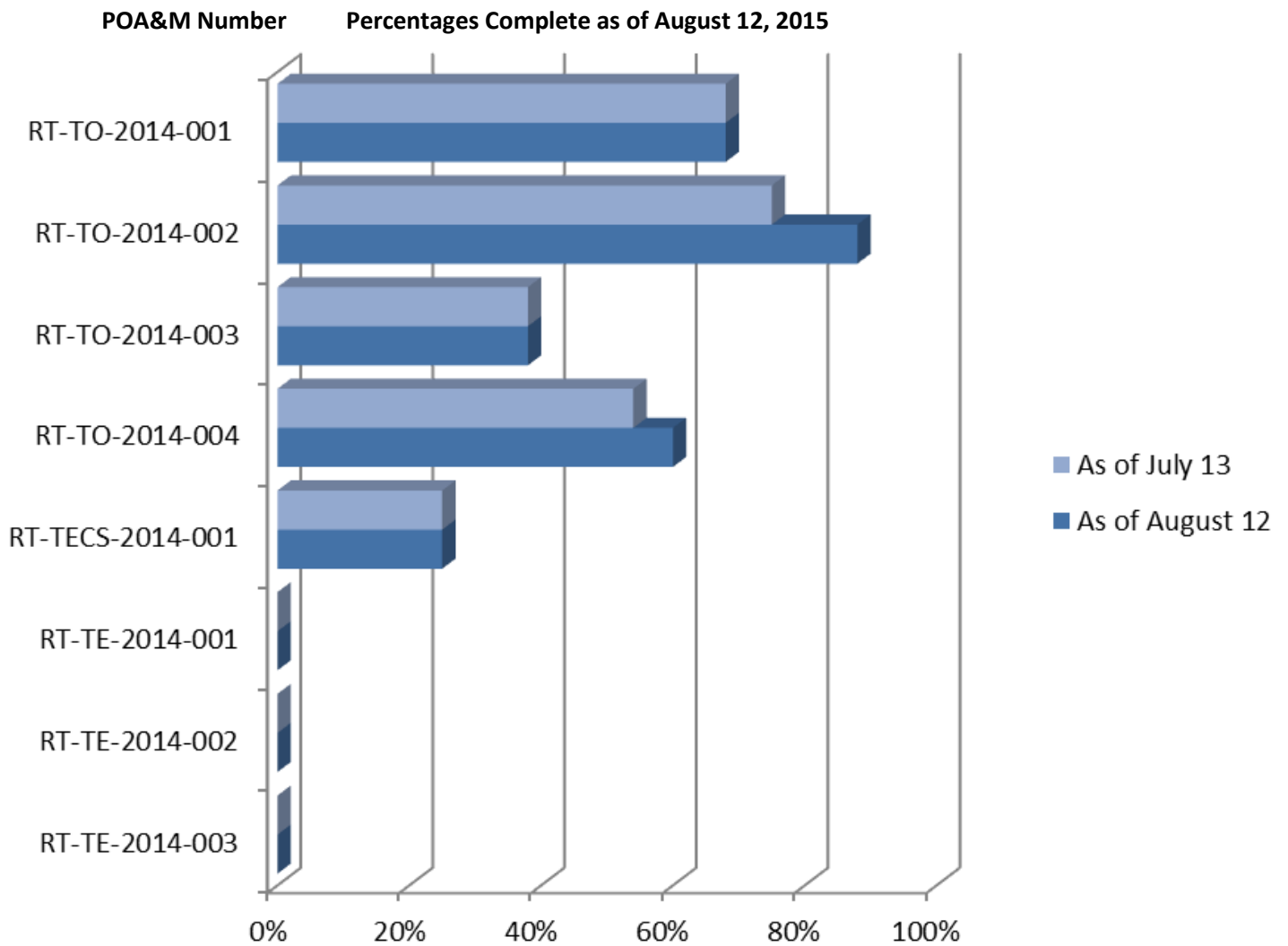
Evaluate and document domain
trusts and FW rules between
various environments

Work Scheduled to Begin Later:

Evaluate and document domain
trusts and FW rules between Grid
Ops and IT Ops; Implement new
FW rule configurations

POA&M Percent Complete for Transmission

Mitigation Activities for Transmission, for TO, TEC, and TC combined, are 35% Complete



POA&M Details for Transmission

(no change in progress since the last report)

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M	Remediation Tasks	Progress Updates	Team
RT-TO-2014-001	<p>Work Completed: Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable</p> <p>Work in Progress: Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire; due, Sept 30, 2015.</p>	(no progress since last report)	Andy McDonald, John Mare
RT-TO-2014-002	<p>Work Completed: Evaluate DGOZ GOPs to ensure only privileged roles can run executable files; The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution</p> <p>Work in Progress: Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions; due Sept 30, 2015.</p>	Updated Work in Progress: LANDesk HIPS solution has been evaluated; due Sept 30, 2015.	Andy McDonald, John Mare
RT-TO-2014-003	<p>Work Completed: Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) <i>Note: Could only be enforced procedurally</i></p> <p>Work in Progress: Update Windows Account Management Plan to reflect change in standard; due Dec 31, 2015.</p> <ul style="list-style-type: none"> • 16 character service account passwords • 12 character interactive user account passwords 	(no progress since last report)	Andy McDonald, John Mare

Work not Started:

Create and enforce Control Center issue-specific password policy (due 3/31/2015); Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment; due Dec 31, 2015

RT-TO-2014-004

Work in Progress:

Remove the domain trust from BUD to DGOZ; due June 30, 2016 (*Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust; due June 30, 2015 (*Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary; due Dec 31, 2015 (*Note: Relying CIP to provide solution*); Progress was made on resolving competing strategies between the Control Center and Corporate IT

Updated Work in Progress:

CCN has designed the DMZ architecture. However the J team did not approve of the design, and is presently performing a redesign (due June 30, 2016)

Andy McDonald, John Mare

RT-TECS-2014-001
(Scott Lissit)

Work Completed:

Purchase and test secure USBs for use on SPC equipment

(no progress since last report)

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens; all work is due to be completed within 12 months of approved funding date.

RT-TE-2014-001
(unknown)

Work not Started:

Configure files integrity tool (Tripwire) appropriately; Centralized logging of

(no progress since last report)

file integrity activity (Splunk) both tasks
due 1/30/15

RT-TE-2014-002
(unknown)

Work not Started:
Update the system security (SSP) with
authorization boundary and inventory;
due 12/31/2014

(no progress since last
report)

RT-TE-2014-003
(unknown)

Work not Started:
Integrate access control for SPC users
and devices into the OMET plan;
Implement monitoring for SPC devices
to log unsuccessful access attempts.
Add to the OMET plan; due 4/1/2016

(no progress since last
report)

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet

- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms) and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete.....	2
POA&M Percent Complete for IT.....	3
POA&M Details for IT.....	4
POA&M Percent Complete for Transmission.....	14
POA&M Details for Transmission.....	15
Glossary.....	17

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

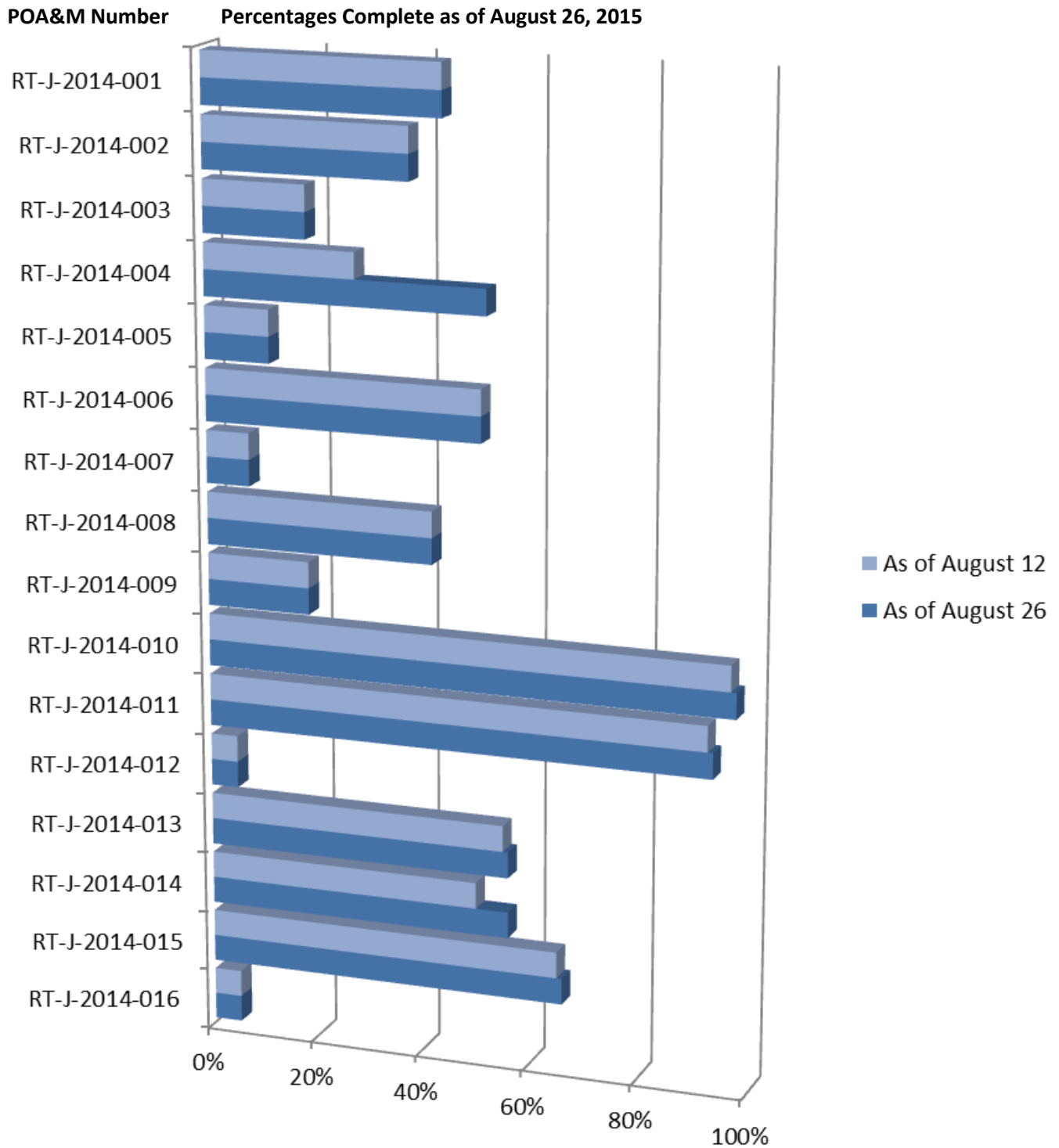
The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

Mitigation activities across all teams, IT and Transmission, are 40% complete

POA&M Percent Complete for IT

Mitigation activities for J, across all POA&Ms, are 41% complete

RT-J-2014-016 was re-evaluated and a new strategy is being developed.



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)	Team
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat (8/7/2015)</p> <p>Work in Progress: Ongoing efforts to remove unnecessary member groups (completion due- 7/31/2015)</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution (completion due- 6/26/2015)</p>		Betty Pedersen, Steve Ireland

RT-J-2014-002

Work Completed:

Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Choose technology for EndPoint Protection Solution; Finish system planning phase for endpoint protection (completion due-3/30/2015);

Work Scheduled to Begin Later:

Implementation for logging at endpoints (10/23/2015); Complete process for leveraging workstation logs as part of event monitoring (10/30/2015); Rollout endpoint protection solution for servers and workstations (10/30/2015)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(logging at endpoints)
Chris Glanville

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing; Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS;

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (Splunk)
Ross Bradley, Chris
Glanville

Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec proof of concept; Cisco FireSight PO leveraged

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology (no date); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Ensure new NIDS logs are ingested by Splunk (no date)

Work not Started:

Finish NIDS system planning phase (no date); Document O&M requirements for NIDS solution(no date); Ensure NIDS logs response procedures are in place (no date)

RT-J-2014-004

Work Completed:

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased; LDAP logging successfully implemented in BRE and IRE

Updated Work Completed:

LDAP logging was successfully implemented in BUD, DRD, and the DMZ

(LDAP event logging on all domain controllers)Chris Glanville, Betty Pedersen, John O'Donnell

Work in Progress:

Build Domain Admin management servers and workstations; (completion due – 6/30/2015); Domain admins transition to using new management servers (completion due – 6/30/2015)

RT-J-2014-005

Work Completed:

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement FIM including logging;
Implement endpoint protection suite incorporating application whitelisting (6/26/2015)

RT-J-2014-006

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated; Completed testing of Trend Micro for endpoint protection, including Application Control ; New VDI group policies for Citrix have been promoted to BRE and IRE environments; Purchase request for new WebSense replacement hardware was submitted; Recommended workstation group policies baseline is complete

Updated Work Completed:

Four legacy group policy objects were retired.

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
Katie Feucht; (Websense)
Jason Enger; (Citrix) Eric
Wilson, Katie Feucht

Work in Progress:

Changes to draft updated Windows 7 standard (12/4/2015); Cleanup workstation group policies (12/4/2015); Cleanup Citrix group policies (7/15/2015); Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Updated Work in Progress:

WebSense appliance installation is in progress in DRE (8/14/2015)

Work Scheduled to Begin Later:

Implement endpoint protection suite incorporating application whitelisting (3/30/2015)

RT-J-2014-007

Work Complete:

Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (web application FW) Chuck Dockery, Jason Enger

Work in Progress:

Make a decision on NIDS technology (no date)

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Implement a Web Application FW (10/2/2015)

RT-J-2014-008

Work Completed:

Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs;

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (Websense) Jason Enger

Websense license upgrade received and successfully installed; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Work in Progress:

Ensure CSOAC receives proper NIDS feeds (no date)

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

Updated Work in Progress:

WebSense appliance installation is in progress in DRE (8/14/2015)

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDs feeds in Splunk; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen

Work Scheduled to Begin Later:
Implement EndPoint protection incorporating Application Whitelisting (3/30/2015); Replace NIDS equipment (no date); Complete NIDs replacement project (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-010

Work Complete:
Tripwire review is complete in the development environment; Added @bpa.gov to “Blacklisted senders;” Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments; Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

Work in Progress:
Creating process for updating Sophos rules (2/27/15)

Updated Work Complete:
Cyber has approved final documentation for Exchange/mail environment; Sophos contract is signed

Darlene Williams, Betty Pedersen

RT-J-2014-011

Work Complete:
Added @bpa.gov to “Blacklisted senders;” Verified that Sophos virus definitions are updated;

Updated Work Complete:
Sophos contract is signed

Darlene Williams, Betty Pedersen

reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management; Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR

Updated Work in Progress:
Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)

RT-J-2014-012

Updated Work Completed:
Finished analyzing difference between current MS Office Policies and latest DISA STIG macro settings

Loyd Towe, Matt Buss, Katie Feucht

Work in Progress:
Update group policies for Office product macros (12/30/2015)

RT-J-2014-013

Work Completed:
Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights; Power settings have been reviewed and updated

Updated Work Completed:
Four legacy group policy objects were retired; SPC laptops are ready for testing; SPC group policy is updated

(Win 7 Policies) Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans; Katie Feucht; (Websense) Jason Enger; (SPC laptops) Loyd Towe, Ken Ballou); (group policies) Betty Pedersen

Work in Progress:
Changes to draft updated Windows 7 standard (12/15/2015); Improve management of SPC laptops (no date); Clean up Citrix group policies (7/15/2015); Enforce group policy change control policies and procedures (4/24/2015)

Updated Work in Progress:
WebSense appliance installation is in progress in DRE (8/14/2015)

RT-J-2014-014

Work Complete:
Update weak passwords; Phase 1 testing in DRE; 12 inactive standard accounts were disabled and scheduled for deletion; Inactive account script updated to better sanitize out of scope accounts; Draft documented process is created; EPU accounts are fully applied in DRE; Password script implementation finalized; Implement password policies for EPU accounts

Updated Work Complete:
Inactive service accounts have all been reviewed, relevant accounts have been disabled or documented as exceptions; 15 character passwords are fully applied to all EPU accounts in BRE and IRE.

(inactive accounts) Betty Pedersen, Steve Ireland; (failed login attempts) Chris Clanville, David, Mullin, Brian Dugan

Work in Progress:
Coordinate with CSOAC to reduce false positives for failed login attempts (5/1/2015); Implement password policies for service accounts (12/30/2015)

Updated Work in Progress:
Review of inactive service accounts is ongoing; Work in Progress to resolve svcSCCMforest failed logons in DRE and BRE environments; Installing latest Splunk agent on RSA servers in DMZ

Work Scheduled to Begin Later:
Submit plan for maintenance of inactive accounts (9/30/2015); Publish account maintenance guidelines to BITA; Select automated tool for account management

RT-J-2014-015

Work Completed:
Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices;

(logging) Chris Clanville, David, Mullin, Brian Dugan

Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; implement process for resolution of future logging support

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives" (5/1/2015); Resolve missing log sources (6/16/2015); Resolve high frequency event tuning (6/19/2015)

Updated Work in Progress:

Work in Progress to resolve svcSCCMforest failed logons in DRE and BRE environments; Installing latest Splunk agent on RSA servers in DMZ

Work Scheduled to Begin Later:

Selection of automated asset inventory tool (no date)

RT-J-2014-016

Work in Progress (but on hold):

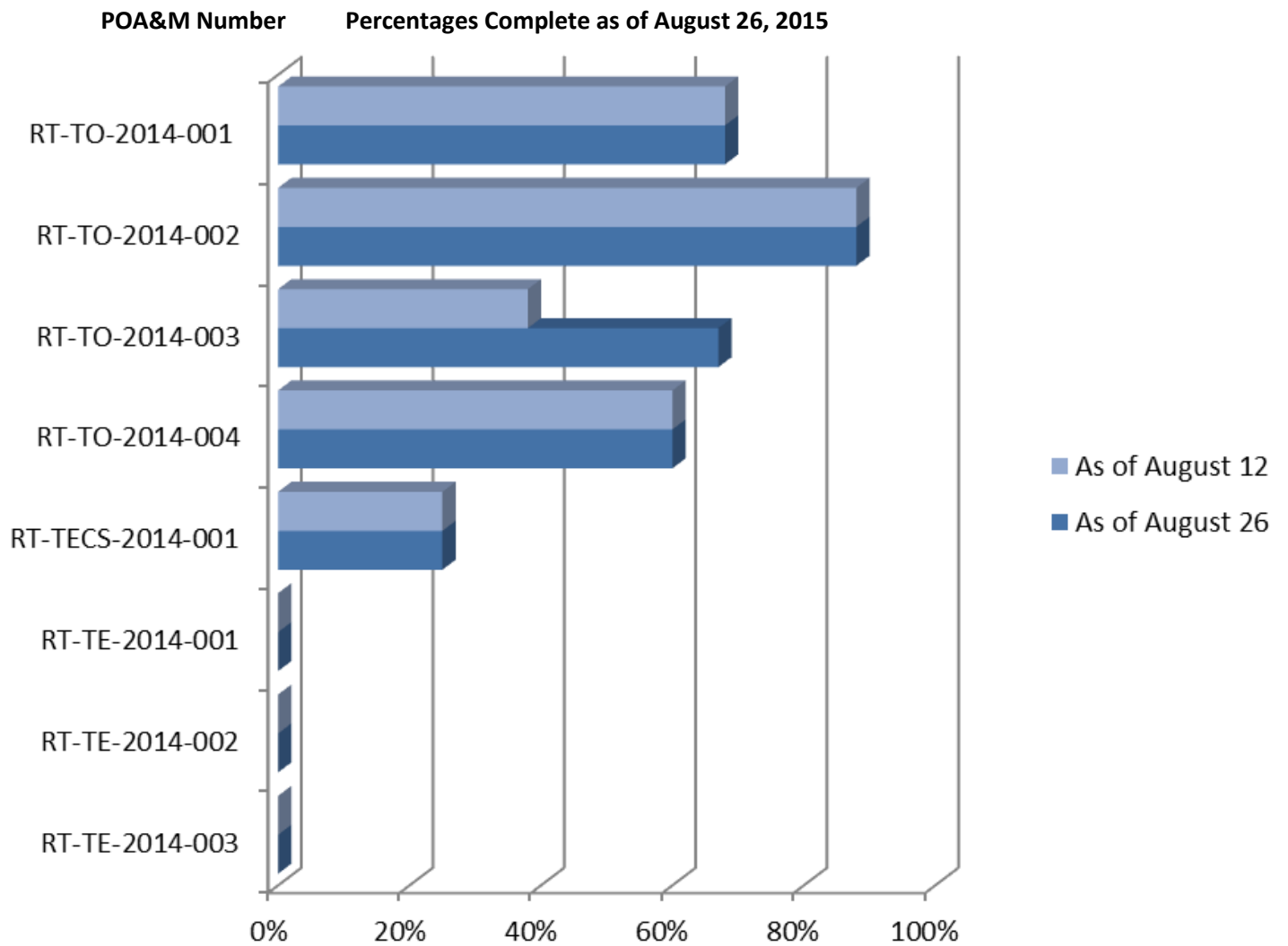
Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

POA&M Percent Complete for Transmission

Mitigation Activities for Transmission, for TO, TEC, and TC combined, are 39% Complete



POA&M Details for Transmission

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M	Remediation Tasks	Progress Updates	Team
RT-TO-2014-001	<p>Work Completed: Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable</p> <p>Work in Progress: Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire (due, Sept 30, 2015.)</p>	(no progress since last report)	Andy McDonald, John Mare
RT-TO-2014-002	<p>Work Completed: Evaluate DGOZ GOPs to ensure only privileged roles can run executable files; The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution</p> <p>Work in Progress: Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions (due Sept 30, 2015.)</p>		Andy McDonald, John Mare
RT-TO-2014-003	<p>Work Completed: Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) <i>Note: Could only be enforced procedurally;</i> Create and enforce Control Center issue-specific password policy</p>	Updated Work Completed: Password length and complexity issue are incorporated into the BITA	Andy McDonald, John Mare, Rustin Jones

Work in Progress:

Update Windows Account Management Plan to reflect change in standard (due Dec 31, 2015.)

- 16 character service account passwords
- 12 character interactive user account passwords

Work not Started:

Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment (due Dec 31, 2015)

RT-TO-2014-004

Work in Progress:

Remove the domain trust from BUD to DGOZ (due June 30, 2016 - *Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (due June 30, 2015 - *Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (due Dec 31, 2015 - *Note: Relying CIP to provide solution*); Progress was made on resolving competing strategies between the Control Center and Corporate IT

(no progress since last report)

Andy McDonald, John Mare

RT-TECS-2014-001
(Scott Lissit)

Work Completed:

Purchase and test secure USBs for use on SPC equipment

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens; all work is due to be completed within 12 months of approved funding date.

(no progress since last report)

RT-TE-2014-001 (unknown)	Work not Started: Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk) (both tasks due 1/30/15)	(no progress since last report)
RT-TE-2014-002 (unknown)	Work not Started: Update the system security (SSP) with authorization boundary and inventory (due 12/31/2014)	(no progress since last report)
RT-TE-2014-003 (unknown)	Work not Started: Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan (due 4/1/2016)	(no progress since last report)

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively

developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.

- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms) and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete.....	2
POA&M Percent Complete for IT.....	3
POA&M Details for IT.....	4
POA&M Percent Complete for Transmission.....	14
POA&M Details for Transmission.....	15
Glossary.....	17

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

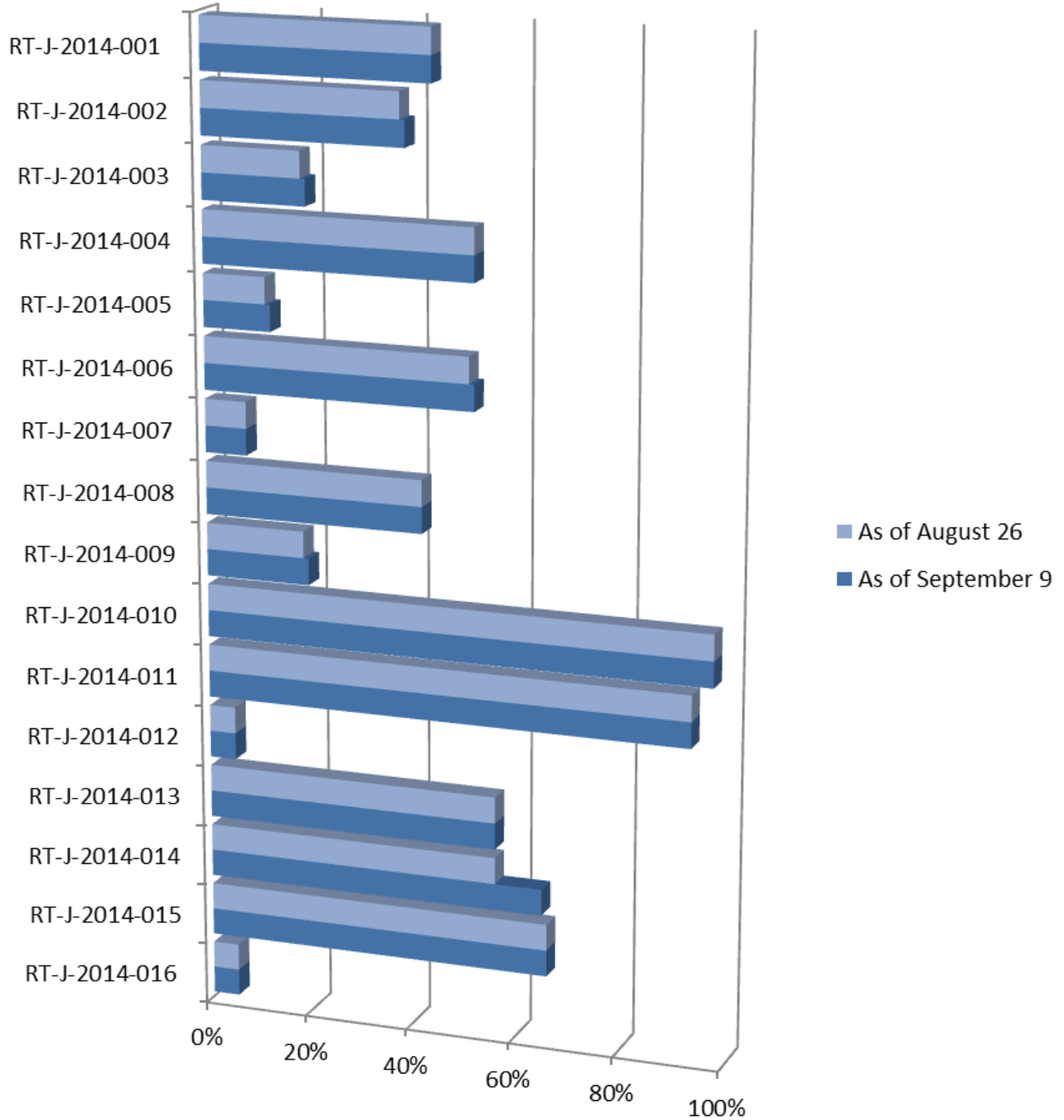
Mitigation activities across all teams, IT and Transmission, are 41% complete

POA&M Percent Complete for IT (J)

Mitigation activities for J, across all POA&Ms, are 42% complete

RT-J-2014-016 was re-evaluated and a new strategy is being developed.

POA&M Number Percentages Complete as of September 9, 2015



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)	Team
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat (8/7/2015)</p> <p>Work in Progress: Ongoing efforts to remove unnecessary member groups (completion due- 7/31/2015)</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution (completion due- 6/26/2015)</p>	(no progress since last report)	Betty Pedersen, Steve Ireland

RT-J-2014-002

Work Completed:

Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015);

Work Scheduled to Begin Later:

Implementation for logging at endpoints (10/23/2015); Complete process for leveraging workstation logs as part of event monitoring (10/30/2015); Rollout endpoint protection solution for servers and workstations (10/30/2015)

Updated Work Complete:

Selection of Symantec for endpoint protection tool

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(logging at endpoints)
Chris Glanville

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing; Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS;

Updated Work Complete:

Selection of Symantec for endpoint protection tool

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (Splunk)
Ross Bradley, Chris
Glanville

Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec proof of concept; Cisco FireSight PO leveraged

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology (no date); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Ensure new NIDS logs are ingested by Splunk (no date)

Work not Started:

Finish NIDS system planning phase (no date); Document O&M requirements for NIDS solution(no date); Ensure NIDS logs response procedures are in place (no date)

RT-J-2014-004

Work Completed:

Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased; LDAP logging successfully implemented in BRE and IRE

(no progress since last report)

(LDAP event logging on all domain controllers)Chris Glanville, Betty Pedersen, John O'Donnell

Work in Progress:

Build Domain Admin management servers and workstations; (completion due – 6/30/2015); Domain admins transition to using new management servers (completion due – 6/30/2015)

RT-J-2014-005

Work Completed:

Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control

Updated Work Complete:

Selection of Symantec for endpoint protection tool

Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement FIM including logging;
Implement endpoint protection suite incorporating application whitelisting (6/26/2015)

RT-J-2014-006

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on firewalls (FWs); Configure Web Cache Communications Protocol (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated; Completed testing of Trend Micro for endpoint protection, including Application Control ; New VDI group policies for Citrix have been promoted to BRE and IRE environments; Purchase request for new WebSense replacement hardware was submitted;

Updated Work Complete:

Selection of Symantec for endpoint protection tool; COG approved the group policy baseline

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
Katie Feucht; (Websense)
Jason Enger; (Citrix) Eric
Wilson, Katie Feucht

workstation group policies
baseline is complete

Work in Progress:

Changes to draft updated
Windows 7 standard (12/4/2015);
Cleanup workstation group
policies (12/4/2015); **Cleanup
Citrix group policies (7/15/2015);
Finish system planning phase for
endpoint protection (completion
due- 3/30/2015)**

Work Scheduled to Begin Later:

**Implement endpoint protection
suite incorporating application
whitelisting (3/30/2015)**

RT-J-2014-007

Work Complete:

Review Cisco support contract for
NIDS, ensuring receipt of new
signatures; Ensure CSOAC is
receiving NIDS feeds; Resolve
versioning conflict between NIDS
and Splunk

(no progress since last report)

(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (web
application FW) Chuck
Dockery, Jason Enger

Work in Progress:

**Make a decision on NIDS
technology (no date)**

Work Scheduled to Begin Later:

**Replace NIDS equipment (no
date); Implement a Web
Application FW (10/2/2015)**

RT-J-2014-008

Work Completed:

Renew FW contract; Remove
unnecessary ports from internal IP
to external IP FW rules; Renew
Cisco contract for NIDS ensure
receipt of new signatures; Resolve
versioning conflict between NIDS
and Splunk; Configure WCCP to
ensure web traffic from myPC
goes through WebSense; HQ
firewalls are successfully
upgraded. Upgrade Check Point
FWs to most recent version;
Replace perimeter Check Point
FWs;

(no progress since last report)

(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (Websense)
Jason Enger

Websense license upgrade received and successfully installed; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Work in Progress:

Ensure CSOAC receives proper NIDS feeds (no date)

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDs feeds in Splunk; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Updated Work Complete:

Selection of Symantec for endpoint protection tool

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen

Work Scheduled to Begin Later:
Implement EndPoint protection incorporating Application Whitelisting (3/30/2015); Replace NIDS equipment (no date); Complete NIDs replacement project (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-010

Work Complete:
Tripwire review is complete in the development environment; Added @bpa.gov to “Blacklisted senders;” Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments; Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

Work in Progress:
Creating process for updating Sophos rules (2/27/15); Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)

(no progress since last report)

Darlene Williams, Betty Pedersen

RT-J-2014-011	<p>Work Complete: Added @bpa.gov to “Blacklisted senders;” Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JN1 is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management; Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR</p> <p>Work in Progress: Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)</p>	(no progress since last report)	Darlene Williams, Betty Pedersen
RT-J-2014-012	<p>Updated Work Completed: Finished analyzing difference between current MS Office Policies and latest DISA STIG macro settings</p> <p>Work in Progress: Update group policies for Office product macros (12/30/2015)</p>	(no progress since last report)	Loyd Towe, Matt Buss, Katie Feucht
RT-J-2014-013	<p>Work Completed: Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights;</p>	Updated Work Completed: COG approved the group policy baseline	(Win 7 Policies) Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans; Katie Feucht; (Websense) Jason Enger; (SPC laptops) Loyd Towe, Ken Ballou); (group policies) Betty Pedersen

Power settings have been reviewed and updated; SPC group policy is updated

Work in Progress:

Changes to draft updated Windows 7 standard (12/15/2015); **Improve management of SPC laptops (no date); Clean up Citrix group policies (7/15/2015); Enforce group policy change control policies and procedures (4/24/2015)**

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE; 12 inactive standard accounts were disabled and scheduled for deletion; Inactive account script updated to better sanitize out of scope accounts; Draft documented process is created; EPU accounts are fully applied in DRE; Password script implementation finalized; Implement password policies for EPU accounts; Inactive service accounts have all been reviewed, relevant accounts have been disabled or documented as exceptions

Work in Progress:

Coordinate with CSOAC to reduce false positives for failed login attempts (5/1/2015); Implement password policies for service accounts (12/30/2015)

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts (9/30/2015); Publish account maintenance guidelines to BITA; Select automated tool for account management

Updated Work Complete:

15 character passwords are fully applied to all EPU accounts in BUD.

(inactive accounts) Betty Pedersen, Steve Ireland; (failed login attempts) Chris Clanville, David, Mullin, Brian Dugan

Updated Work in Progress:

Work continues on clean-up of inactive service accounts

RT-J-2014-015 **Work Completed:** **(no progress since last report)** (logging) Chris Clanville, David, Mullin, Brian Dugan

Coordinate with CSOAC to resolve Exchange logging problems;
Obtain list of missing log sources;
Resolve improperly parsed logs;
Evaluate high frequency events for tuning;
Implement automated inventory of authorized and unauthorized devices;
Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; implement process for resolution of future logging support

Work in Progress:
Work with CSOAC to reduce “failed login” attempts “false positives” (5/1/2015); Resolve missing log sources (6/16/2015); Resolve high frequency event tuning (6/19/2015)

Work Scheduled to Begin Later:
Selection of automated asset inventory tool (no date)

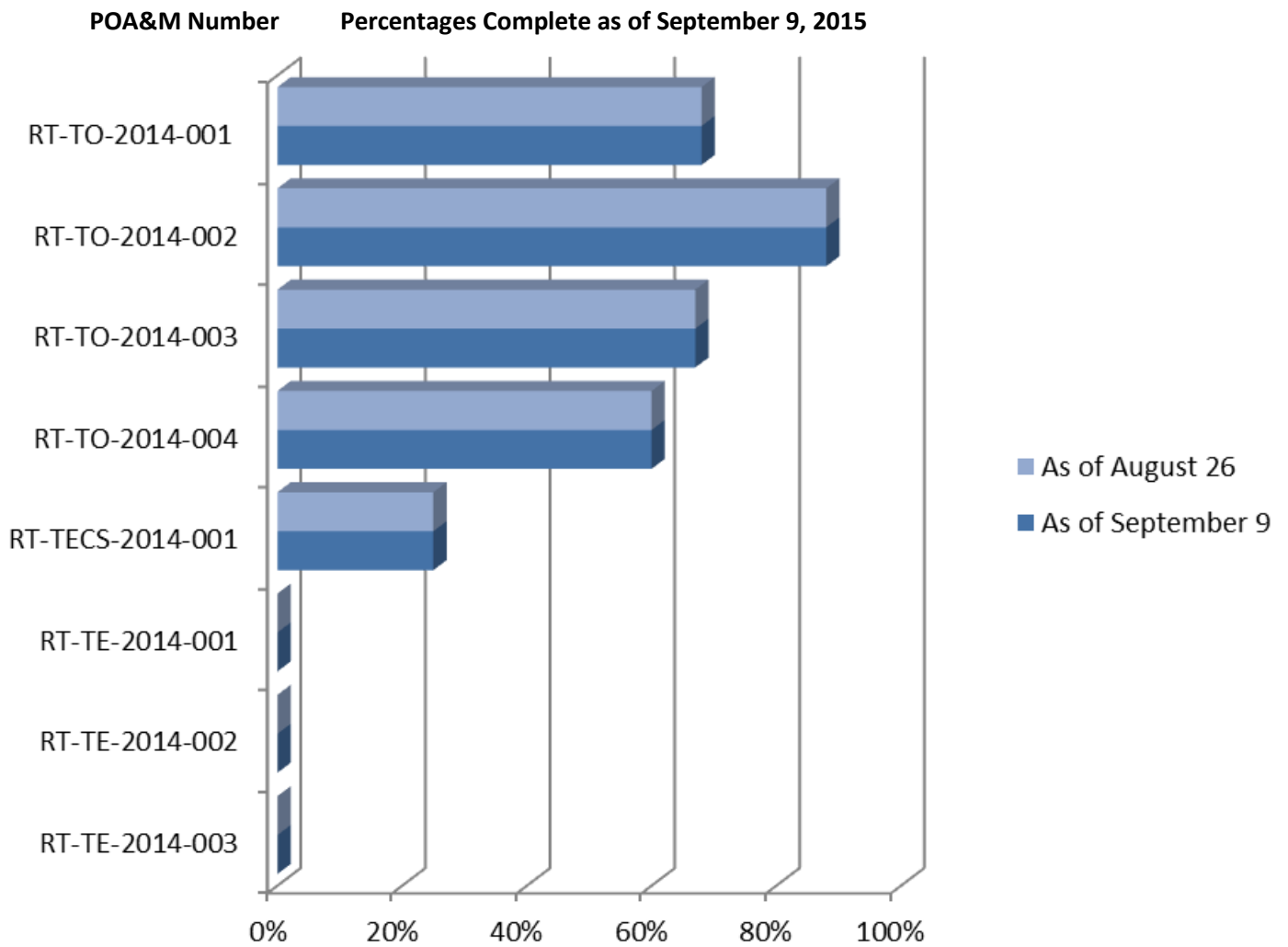
RT-J-2014-016 **Work in Progress (but on hold):** **(no progress since last report)**

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:
Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

POA&M Percent Complete for Transmission

Mitigation Activities for Transmission, for TO, TEC, and TC combined, are 39% Complete



POA&M Details for Transmission

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M	Remediation Tasks	Progress Updates	Team
RT-TO-2014-001	<p>Work Completed: Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable</p> <p>Work in Progress: Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire (due, Sept 30, 2015.)</p>	(no progress since last report)	Andy McDonald, John Mare
RT-TO-2014-002	<p>Work Completed: Evaluate DGOZ GOPs to ensure only privileged roles can run executable files; The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution</p> <p>Work in Progress: Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions (due Sept 30, 2015.)</p>	(no progress since last report)	Andy McDonald, John Mare
RT-TO-2014-003	<p>Work Completed: Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) <i>Note: Could only be enforced procedurally;</i> Create and enforce Control Center issue-specific password policy; Password length and complexity issue are incorporated into the BITA</p>	(no progress since last report)	Andy McDonald, John Mare, Rustin Jones

Work in Progress:

Update Windows Account Management Plan to reflect change in standard (due Dec 31, 2015.)

- 16 character service account passwords
- 12 character interactive user account passwords

Work not Started:

Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment (due Dec 31, 2015)

RT-TO-2014-004

Work in Progress:

Remove the domain trust from BUD to DGOZ (due June 30, 2016 - *Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (due June 30, 2015 - *Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (due Dec 31, 2015 - *Note: Relying CIP to provide solution*); Progress was made on resolving competing strategies between the Control Center and Corporate IT

(no progress since last report)

Andy McDonald, John Mare

RT-TECS-2014-001
(Scott Lissit)

Work Completed:

Purchase and test secure USBs for use on SPC equipment

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens; all work is due to be completed within 12 months of approved funding date.

(no progress since last report)

RT-TE-2014-001
(unknown)

Work not Started:
Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk) (both tasks due 1/30/15)

(no progress since last report)

RT-TE-2014-002
(unknown)

Work not Started:
Update the system security (SSP) with authorization boundary and inventory (due 12/31/2014)

(no progress since last report)

RT-TE-2014-003
(unknown)

Work not Started:
Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan (due 4/1/2016)

(no progress since last report)

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.

- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.
- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms) and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete.....	2
POA&M Percent Complete for IT.....	3
POA&M Details for IT.....	4
POA&M Percent Complete for Transmission.....	15
POA&M Details for Transmission.....	16
Glossary.....	18

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

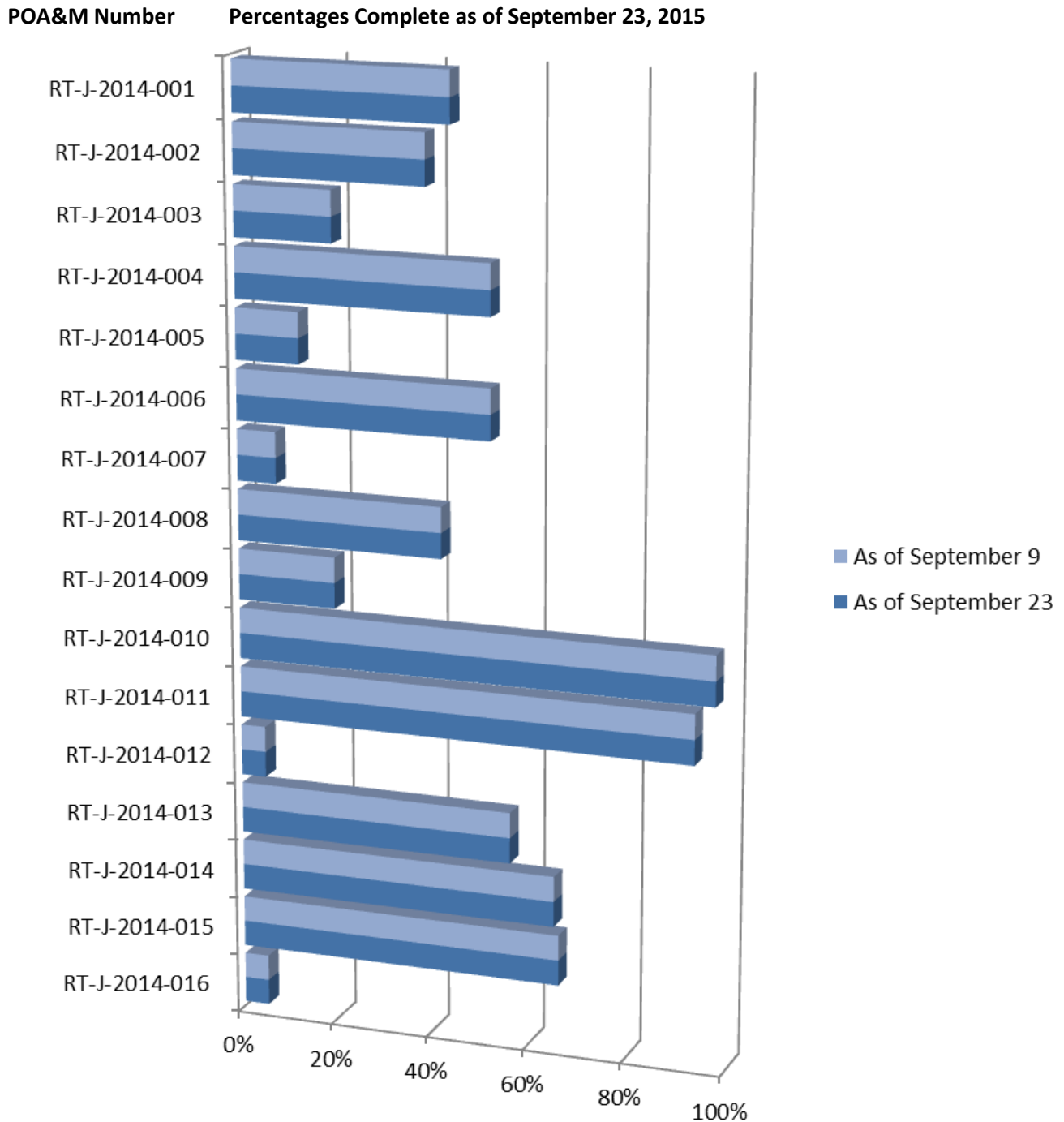
The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

Mitigation activities across all teams, IT and Transmission, are 41% complete

POA&M Percent Complete for IT (J)

Mitigation activities for J, across all POA&Ms, have not progressed since the last report. The percentages complete remain at 42%.

RT-J-2014-016 was re-evaluated and a new strategy is being developed.



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)	Team
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat (8/7/2015)</p> <p>Work in Progress: Ongoing efforts to remove unnecessary member groups (completion due- 7/31/2015)</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution (completion due- 6/26/2015)</p>	(no progress since last report)	Betty Pedersen, Steve Ireland

RT-J-2014-002

Work Completed:

Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control; Selection of Symantec for end-point protection tool

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015);

Work Scheduled to Begin Later:

Implementation for logging at endpoints (10/23/2015); Complete process for leveraging workstation logs as part of event monitoring (10/30/2015); Rollout endpoint protection solution for servers and workstations (10/30/2015)

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(logging at endpoints)
Chris Glanville

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing; Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec proof of concept; Cisco FireSight PO leveraged; Selection of Symantec for end-point protection tool

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Lloyd Towe, Pete Albert,
Chris Glanville, Earl Evans
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (Splunk)
Ross Bradley, Chris
Glanville

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology (no date); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Ensure new NIDS logs are ingested by Splunk (no date)

Work not Started:

Finish NIDS system planning phase (no date); Document O&M requirements for NIDS solution(no date); Ensure NIDS logs response procedures are in place (no date)

RT-J-2014-004 **Work Completed:** **(no progress since last report)** (LDAP event logging on all domain controllers)Chris Glanville, Betty Pedersen, John O'Donnell
Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased; LDAP logging successfully implemented in BRE and IRE

Work in Progress:
Build Domain Admin management servers and workstations; (completion due – 6/30/2015); Domain admins transition to using new management servers (completion due – 6/30/2015)

RT-J-2014-005 **Work Completed:** **(no progress since last report)** Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans
Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control; Selection of Symantec for end-point protection tool

Work in Progress:
Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:
Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting (6/26/2015)

RT-J-2014-006

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated; Completed testing of Trend Micro for endpoint protection, including Application Control ; New VDI group policies for Citrix have been promoted to BRE and IRE environments; Purchase request for new WebSense replacement hardware was submitted;

workstation group policies baseline is complete; Selection of Symantec for end-point protection tool; COG approved the group policy baseline

Work in Progress:

Changes to draft updated Windows 7 standard (12/4/2015); Cleanup workstation group policies (12/4/2015); **Cleanup Citrix group policies (7/15/2015);**

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
Katie Feucht; (Websense)
Jason Enger; (Citrix) Eric
Wilson, Katie Feucht

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:
Implement endpoint protection suite incorporating application whitelisting (3/30/2015)

RT-J-2014-007

Work Complete:
Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk

(no progress since last report)

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (web application FW) Chuck Dockery, Jason Enger

Work in Progress:
Make a decision on NIDS technology (no date)

Work Scheduled to Begin Later:
Replace NIDS equipment (no date); Implement a Web Application FW (10/2/2015)

RT-J-2014-008

Work Completed:
Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Websense license upgrade received and successfully installed; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS;

(no progress since last report)

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (Websense) Jason Enger

A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Work in Progress:

Ensure CSOAC receives proper NIDS feeds (no date)

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDs feeds in Splunk; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control; Selection of Symantec for end-point protection tool

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting (3/30/2015); Replace NIDS equipment (no date); Complete NIDs replacement project (no date);

Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments; Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

(no progress since last report)

Darlene Williams, Betty Pedersen

Work in Progress:

Creating process for updating Sophos rules (2/27/15); Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JN1 is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management;

(no progress since last report)

Darlene Williams, Betty Pedersen

Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR

Work in Progress:

Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)

RT-J-2014-012

Updated Work Completed:

Finished analyzing difference between current MS Office Policies and latest DISA STIG macro settings

(no progress since last report)

Loyd Towe, Matt Buss, Katie Feucht

Work in Progress:

Update group policies for Office product macros (12/30/2015)

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights; Power settings have been reviewed and updated; SPC group policy is updated

(no progress since last report)

(Win 7 Policies) Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans; Katie Feucht; (Websense) Jason Enger; (SPC laptops) Loyd Towe, Ken Ballou); (group policies) Betty Pedersen

Work in Progress:

Changes to draft updated Windows 7 standard (12/15/2015); Improve management of SPC laptops (no date); Clean up Citrix group policies (7/15/2015);

Enforce group policy change
control policies and procedures
(4/24/2015)

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE; 12 inactive standard accounts were disabled and scheduled for deletion; Inactive account script updated to better sanitize out of scope accounts; Draft documented process is created; EPU accounts are fully applied in DRE; Password script implementation finalized; Implement password policies for EPU accounts; Inactive service accounts have all been reviewed, relevant accounts have been disabled or documented as exceptions; 15 character passwords are fully applied to all EPU accounts in BUD. 100% of accounts reviewed and disabled or documented as exceptions

Work in Progress:

Coordinate with CSOAC to reduce false positives for failed login attempts (5/1/2015); Implement password policies for service accounts (12/30/2015)

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts (9/30/2015); Publish account maintenance guidelines to BITA; Select automated tool for account management

Updated Work Complete:

100% of accounts reviewed and disabled or documented as exceptions

(inactive accounts) Betty Pedersen, Steve Ireland; (failed login attempts) Chris Clanville, David, Mullin, Brian Dugan

Updated Work in Progress:

Work continues to troubleshoot connections between Splunk infrastructure and RSA servers in DMZ; SCCM team and Domain admins implementing changes to SCCM architecture to decrease errors causing failed logging for SCCM service accounts

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices;

(no progress since last report)

(logging) Chris Clanville, David, Mullin, Brian Dugan

Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; implement process for resolution of future logging support

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives" (5/1/2015); Resolve missing log sources (6/16/2015); Resolve high frequency event tuning (6/19/2015)

Work Scheduled to Begin Later:

Selection of automated asset inventory tool (no date)

Updated Work in Progress:

Work continues to troubleshoot connections between Splunk infrastructure and RSA servers in DMZ; SCCM team and Domain admins implementing changes to SCCM architecture to decrease errors causing failed logging for SCCM service accounts

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

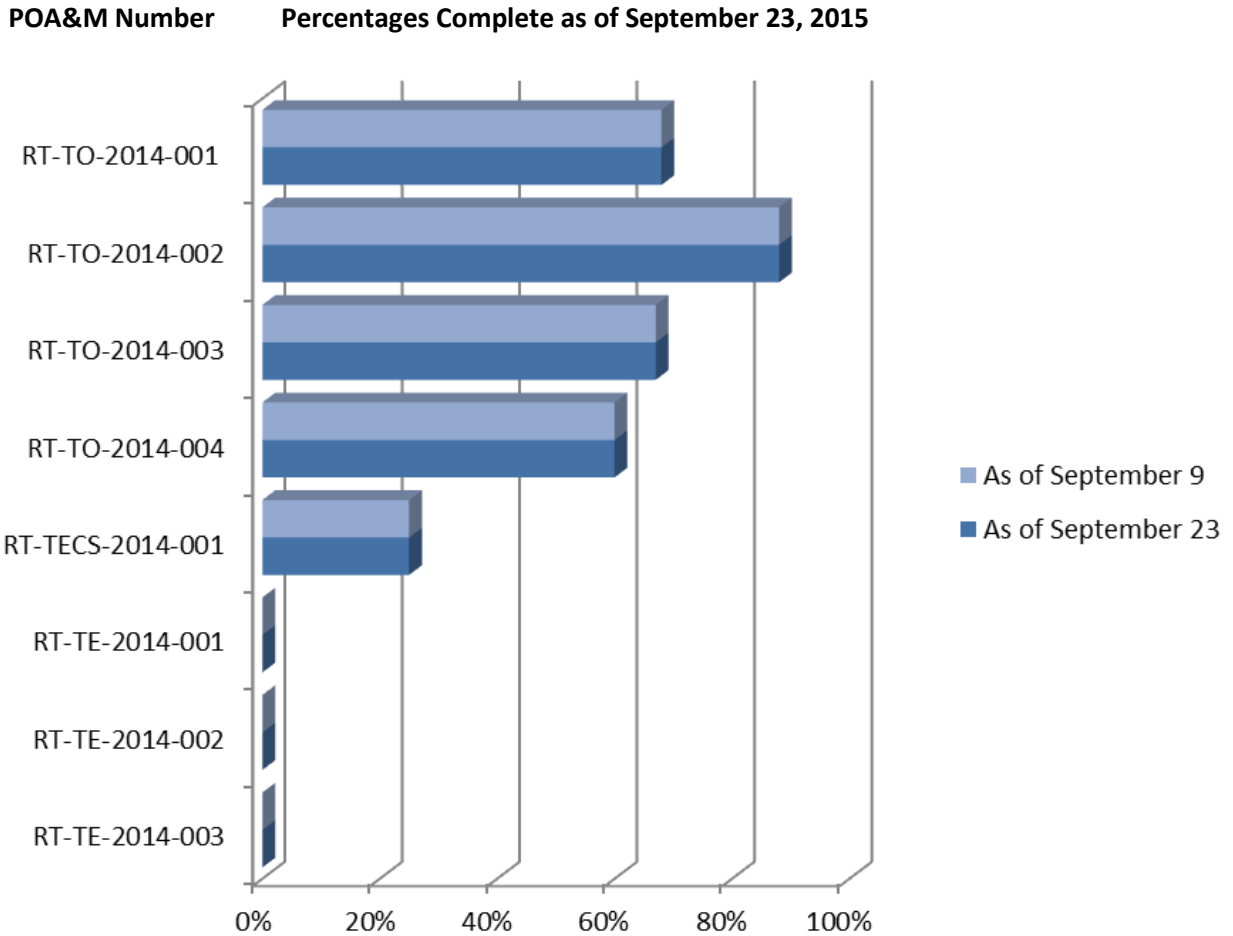
Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

(no progress since last report)

POA&M Percent Complete for Transmission

Mitigation Activities for Transmission, for TO, TEC, and TC combined, have not progressed for one month.

The percentage complete remain at 39% Complete



POA&M Details for Transmission

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M	Remediation Tasks	Progress Updates	Team
RT-TO-2014-001	<p>Work Completed: Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable</p> <p>Work in Progress: Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire (due, Sept 30, 2015.)</p>	(no progress for one month)	Andy McDonald, John Mare
RT-TO-2014-002	<p>Work Completed: Evaluate DGOZ GOPs to ensure only privileged roles can run executable files; The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution</p> <p>Work in Progress: Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions (due Sept 30, 2015.)</p>	(no progress for one month)	Andy McDonald, John Mare
RT-TO-2014-003	<p>Work Completed: Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) <i>Note: Could only be enforced procedurally;</i> Create and enforce Control Center issue-specific password policy; Password length and complexity issue are incorporated into the BITA</p>	(no progress for one month)	Andy McDonald, John Mare, Rustin Jones

Work in Progress:

Update Windows Account Management Plan to reflect change in standard (due Dec 31, 2015.)

- 16 character service account passwords
- 12 character interactive user account passwords

Work not Started:

Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment (due Dec 31, 2015)

RT-TO-2014-004

Work in Progress:

Remove the domain trust from BUD to DGOZ (due June 30, 2016 - *Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (due June 30, 2015 - *Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (due Dec 31, 2015 - *Note: Relying CIP to provide solution*); Progress was made on resolving competing strategies between the Control Center and Corporate IT

(no progress for one month)

Andy McDonald, John Mare

RT-TECS-2014-001
(Scott Lissit)

Work Completed:

Purchase and test secure USBs for use on SPC equipment

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens; all work is due to be completed within 12 months of approved funding date.

(no progress for one month)

RT-TE-2014-001 (unknown)	Work not Started: Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk) (both tasks due 1/30/15)	(no progress for one month)
RT-TE-2014-002 (unknown)	Work not Started: Update the system security (SSP) with authorization boundary and inventory (due 12/31/2014)	(no progress for one month)
RT-TE-2014-003 (unknown)	Work not Started: Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan (due 4/1/2016)	(no progress for one month)

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft

Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.

- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

Red Team Vulnerability Remediation Report

In April 2014, the BPA Office of Cyber Security began an Advanced Persistent Threat (APT) exercise from the Internet with the goal of compromising BPA’s mission critical functions.

This exercise was conducted as a *red team* activity in order to determine how well BPA mission, systems and personnel are protected from external cyber-attacks. The Team’s objectives were BPA’s mission critical systems.

This report is issued bi-monthly and details progress made on the remediation of findings resulting from the *red team* exercise. Each finding is organized into individual *Plans of Action and Milestones* (POA&Ms) and each POA&M consists of multiple tasks that are developed to, as a whole, remediate a particular finding. A task or set of tasks will, in certain cases, address aspects of multiple POA&Ms.

Table of Contents

IT and Transmission Percentages Complete.....	2
POA&M Percent Complete for IT.....	3
POA&M Details for IT.....	4
POA&M Percent Complete for Transmission.....	15
POA&M Details for Transmission.....	16
Glossary.....	18

IT and Transmission Percentages Complete

This report is in two sections. The first section details POA&Ms applicable to the mitigations of vulnerabilities found in IT systems and assets, while the second section refers to those that apply to Transmission systems and assets.

The bar graphs represent the amount of progress completed for each POA&M on the date this report is issued.

The *Percentage Complete* for each POA&M represents a point-in-time estimation. As remediation activities progress the need for additional work may become necessary. Thus, the percentages may vary over time.

The section appearing below the graph outlines each POAM's tasks, and divides tasks into those that are *Complete, In Progress, Not Started, and Scheduled to Begin at a Later Date*.

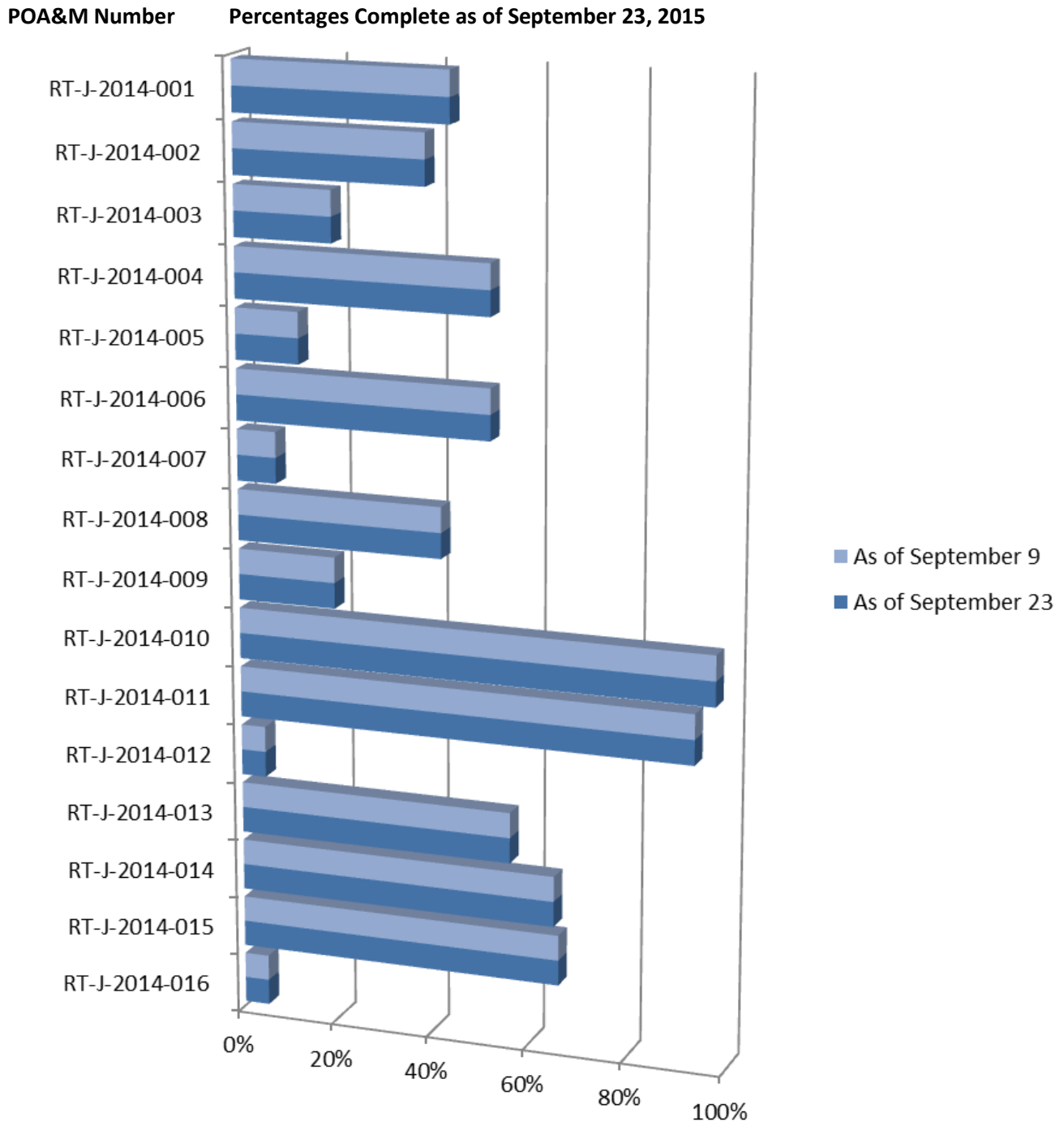
The *Progress Updates* column illustrates which tasks have contributed to the *increased percentage complete*.

Mitigation activities across all teams, IT and Transmission, are 41% complete

POA&M Percent Complete for IT (J)

Mitigation activities for J, across all POA&Ms, have not progressed since the last report. The percentages complete remain at 42%.

RT-J-2014-016 was re-evaluated and a new strategy is being developed.



POA&M Details for IT

Each POA&M or finding from the original Security Assessment Report (SAR) consists of multiple tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates. POAMs with tasks that have slipped past the completion dates (or for which no dates have been agreed upon) are displayed in *red* below:

POA&M	Remediation Tasks (some tasks address multiple POA&Ms)	Progress Updates (tasks updated since last report)	Team
RT-J-2014-001	<p>Work Completed: Update scripts for lan.bat creation; Remove unnecessary settings from startup files; Remove lan.bat modify rights; Update lan.bat permissions; Cleaned up legacy calls; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat; Removed legacy member groups (rscAllServerAdmins Retirement Efforts); Removed unused lan.bat legacy settings; Documented procedures for management of lan.bat (8/7/2015)</p> <p>Work in Progress: Ongoing efforts to remove unnecessary member groups (completion due- 7/31/2015)</p> <p>Work Scheduled to Begin Later: Choose technologies for File Integrity Monitoring (FIM) solution (completion due- 6/26/2015)</p>	(no progress since last report)	Betty Pedersen, Steve Ireland

RT-J-2014-002

Work Completed:

Verify that myPC servers are sending logs to Splunk; Gathering requirements for vendor; specification; Operations staff interviews with vendors; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Choose technology for temp directory whitelisting; installation of TrendMicro software in DRE for testing; Evaluate implementation of AppLocker temp directory; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control; Selection of Symantec for end-point protection tool

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015);

Work Scheduled to Begin Later:

Implementation for logging at endpoints (10/23/2015); Complete process for leveraging workstation logs as part of event monitoring (10/30/2015); Rollout endpoint protection solution for servers and workstations (10/30/2015)

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(logging at endpoints)
Chris Glanville

RT-J-2014-003

Work Completed:

Evaluate implementation of NIDS; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; installation of TrendMicro software in DRE for testing; Installation of TrendMicro software in DRE for testing; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control; Symantec proof of concept; Cisco FireSight PO leveraged; Selection of Symantec for end-point protection tool

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Lloyd Towe, Pete Albert,
Chris Glanville, Earl Evans
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen; (Splunk)
Ross Bradley, Chris
Glanville

Work in Progress:

Requirements gathering for NIDS technology; Choose NIDS technology (no date); Finish system planning phase for endpoint protection (completion due- 3/30/2015); Ensure new NIDS logs are ingested by Splunk (no date)

Work not Started:

Finish NIDS system planning phase (no date); Document O&M requirements for NIDS solution(no date); Ensure NIDS logs response procedures are in place (no date)

RT-J-2014-004 **Work Completed:** **(no progress since last report)** (LDAP event logging on all domain controllers)Chris Glanville, Betty Pedersen, John O'Donnell
Cleanup descriptions of *Elevated Privileges User* (EPU) accounts; Logging level increased; LDAP logging successfully implemented in BRE and IRE

Work in Progress:
Build Domain Admin management servers and workstations; (completion due – 6/30/2015); Domain admins transition to using new management servers (completion due – 6/30/2015)

RT-J-2014-005 **Work Completed:** **(no progress since last report)** Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans
Requirements gathering for endpoint protection; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Completed testing of Trend Micro for endpoint protection, including Application Control; Selection of Symantec for end-point protection tool

Work in Progress:
Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:
Implement FIM including logging; Implement endpoint protection suite incorporating application whitelisting (6/26/2015)

RT-J-2014-006

Work Completed:

Renew FW contract; Remove unnecessary ports from the internal IPs to external IPs FW rule; Update Application Control DB on *firewalls* (FWs); Configure *Web Cache Communications Protocol* (WCCP) for myPC forcing web traffic through WebSense; Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Core license upgrade received and successfully installed; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created. HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Installation of TrendMicro software in DRE for testing; Last comparison analysis between workstation group policies and USGCB has been performed. Power settings have been reviewed and updated; Completed testing of Trend Micro for endpoint protection, including Application Control ; New VDI group policies for Citrix have been promoted to BRE and IRE environments; Purchase request for new WebSense replacement hardware was submitted;

workstation group policies baseline is complete; Selection of Symantec for end-point protection tool; COG approved the group policy baseline

Work in Progress:

Changes to draft updated Windows 7 standard (12/4/2015); Cleanup workstation group policies (12/4/2015); **Cleanup Citrix group policies (7/15/2015);**

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
Katie Feucht; (Websense)
Jason Enger; (Citrix) Eric
Wilson, Katie Feucht

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:
Implement endpoint protection suite incorporating application whitelisting (3/30/2015)

RT-J-2014-007

Work Complete:
Review Cisco support contract for NIDS, ensuring receipt of new signatures; Ensure CSOAC is receiving NIDS feeds; Resolve versioning conflict between NIDS and Splunk

(no progress since last report)

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (web application FW) Chuck Dockery, Jason Enger

Work in Progress:
Make a decision on NIDS technology (no date)

Work Scheduled to Begin Later:
Replace NIDS equipment (no date); Implement a Web Application FW (10/2/2015)

RT-J-2014-008

Work Completed:
Renew FW contract; Remove unnecessary ports from internal IP to external IP FW rules; Renew Cisco contract for NIDS ensure receipt of new signatures; Resolve versioning conflict between NIDS and Splunk; Configure WCCP to ensure web traffic from myPC goes through WebSense; HQ firewalls are successfully upgraded. Upgrade Check Point FWs to most recent version; Replace perimeter Check Point FWs; Websense license upgrade received and successfully installed; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS;

(no progress since last report)

(NIDS) Chuck Dockery, Chris Glanville, Jeff Aske, Jason Enger, Dan Green, David Mullen; (Websense) Jason Enger

A contract has been awarded to Assurance Data for Websense appliances relevant to the Websense upgrade.

Work in Progress:

Ensure CSOAC receives proper NIDS feeds (no date)

Work Scheduled to Begin Later:

Replace NIDS equipment (no date); Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-009

Work Complete:

Requirements Gathering is complete; Renew Cisco contract for NIDS, ensuring receipt of new signatures: Firewall changes made in DRE to allow testing of Trend Micro servers communications with each other; Installation of TrendMicro software in DRE for testing; Complete working with CSOAC concerning NIDs feeds in Splunk; IT Ops Board approved purchase of Cisco FireSIGHT Management Console for Cisco FirePower NIPS; IVC ASAs are licensed for FirePower NIPS; Completed testing of Trend Micro for endpoint protection, including Application Control; Selection of Symantec for end-point protection tool

(no progress since last report)

(endpoint protection)
Aurthur Bendetti-White,
Loyd Towe, Pete Albert,
Chris Glanville, Earl Evans;
(NIDS) Chuck Dockery,
Chris Glanville, Jeff Aske,
Jason Enger, Dan Green,
David Mullen

Work in Progress:

Finish system planning phase for endpoint protection (completion due- 3/30/2015)

Work Scheduled to Begin Later:

Implement EndPoint protection incorporating Application Whitelisting (3/30/2015); Replace NIDS equipment (no date); Complete NIDs replacement project (no date);

Ensure new NIDS logs are ingested by Splunk, and proper CSOAC procedures are in place (no date)

RT-J-2014-010

Work Complete:

Tripwire review is complete in the development environment; Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; Reviewed and created recommendations of whitelisting functionality for Sophos; Ensure Exchange sends logs to Splunk; Finished cleanup of external firewall rules concerning mail traffic on Check Point fire walls; Removed unnecessary objects and organized traffic flows; Full review of Exchange environment; Purchased Exchange App for Splunk ; Tripwire monitoring of approved Exchange baseline is occurring in all environments; Confirmed that Tripwire monitoring of approved Exchange baseline is occurring in all environments

(no progress since last report)

Darlene Williams, Betty Pedersen

Work in Progress:

Creating process for updating Sophos rules (2/27/15); Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)

RT-J-2014-011

Work Complete:

Added @bpa.gov to "Blacklisted senders;" Verified that Sophos virus definitions are updated; reviewed and created recommendations for Sophos whitelisting functionality; Requirements Gathering is complete for email gateway; Management of Sophos from JNN to JNI is complete; HW lifespan review is complete; Exchange admins are trained on Sophos management;

(no progress since last report)

Darlene Williams, Betty Pedersen

Removed DLP task, since a decision was made that the DLP effort does not directly address the RT SAR

Work in Progress:

Cleanup of whitelisted hosts and senders lists relevant to Office macro attachment whitelist (no date)

RT-J-2014-012

Updated Work Completed:

Finished analyzing difference between current MS Office Policies and latest DISA STIG macro settings

(no progress since last report)

Loyd Towe, Matt Buss, Katie Feucht

Work in Progress:

Update group policies for Office product macros (12/30/2015)

RT-J-2014-013

Work Completed:

Local Admin accounts have been moved to a new OU structure, including WebSense blocking Internet access; Configure WCCP to force web traffic from myPC network through WebSense; Tighten group policy change control procedures; Changes to draft updated Windows 7 USGCB baseline; Test workstation created; New SPC OU structure in Bud finished with new SPC group policy linked; Evaluating SPC Admin group rights; Power settings have been reviewed and updated; SPC group policy is updated

(no progress since last report)

(Win 7 Policies) Aurthur Bendetti-White, Loyd Towe, Pete Albert, Chris Glanville, Earl Evans; Katie Feucht; (Websense) Jason Enger; (SPC laptops) Loyd Towe, Ken Ballou); (group policies) Betty Pedersen

Work in Progress:

Changes to draft updated Windows 7 standard (12/15/2015); Improve management of SPC laptops (no date); Clean up Citrix group policies (7/15/2015);

Enforce group policy change
control policies and procedures
(4/24/2015)

RT-J-2014-014

Work Complete:

Update weak passwords; Phase 1 testing in DRE; 12 inactive standard accounts were disabled and scheduled for deletion; Inactive account script updated to better sanitize out of scope accounts; Draft documented process is created; EPU accounts are fully applied in DRE; Password script implementation finalized; Implement password policies for EPU accounts; Inactive service accounts have all been reviewed, relevant accounts have been disabled or documented as exceptions; 15 character passwords are fully applied to all EPU accounts in BUD. 100% of accounts reviewed and disabled or documented as exceptions

Work in Progress:

Coordinate with CSOAC to reduce false positives for failed login attempts (5/1/2015); Implement password policies for service accounts (12/30/2015)

Work Scheduled to Begin Later:

Submit plan for maintenance of inactive accounts (9/30/2015); Publish account maintenance guidelines to BITA; Select automated tool for account management

Updated Work Complete:

100% of accounts reviewed and disabled or documented as exceptions

(inactive accounts) Betty Pedersen, Steve Ireland; (failed login attempts) Chris Clanville, David, Mullin, Brian Dugan

Updated Work in Progress:

Work continues to troubleshoot connections between Splunk infrastructure and RSA servers in DMZ; SCCM team and Domain admins implementing changes to SCCM architecture to decrease errors causing failed logging for SCCM service accounts

RT-J-2014-015

Work Completed:

Coordinate with CSOAC to resolve Exchange logging problems; Obtain list of missing log sources; Resolve improperly parsed logs; Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices;

(no progress since last report)

(logging) Chris Clanville, David, Mullin, Brian Dugan

Evaluate high frequency events for tuning; Implement automated inventory of authorized and unauthorized devices; implement process for resolution of future logging support

Work in Progress:

Work with CSOAC to reduce "failed login" attempts "false positives" (5/1/2015); Resolve missing log sources (6/16/2015); Resolve high frequency event tuning (6/19/2015)

Work Scheduled to Begin Later:

Selection of automated asset inventory tool (no date)

Updated Work in Progress:

Work continues to troubleshoot connections between Splunk infrastructure and RSA servers in DMZ; SCCM team and Domain admins implementing changes to SCCM architecture to decrease errors causing failed logging for SCCM service accounts

RT-J-2014-016

Work in Progress (but on hold):

Evaluate and document domain trusts and FW rules between various environments

Work Scheduled to Begin Later:

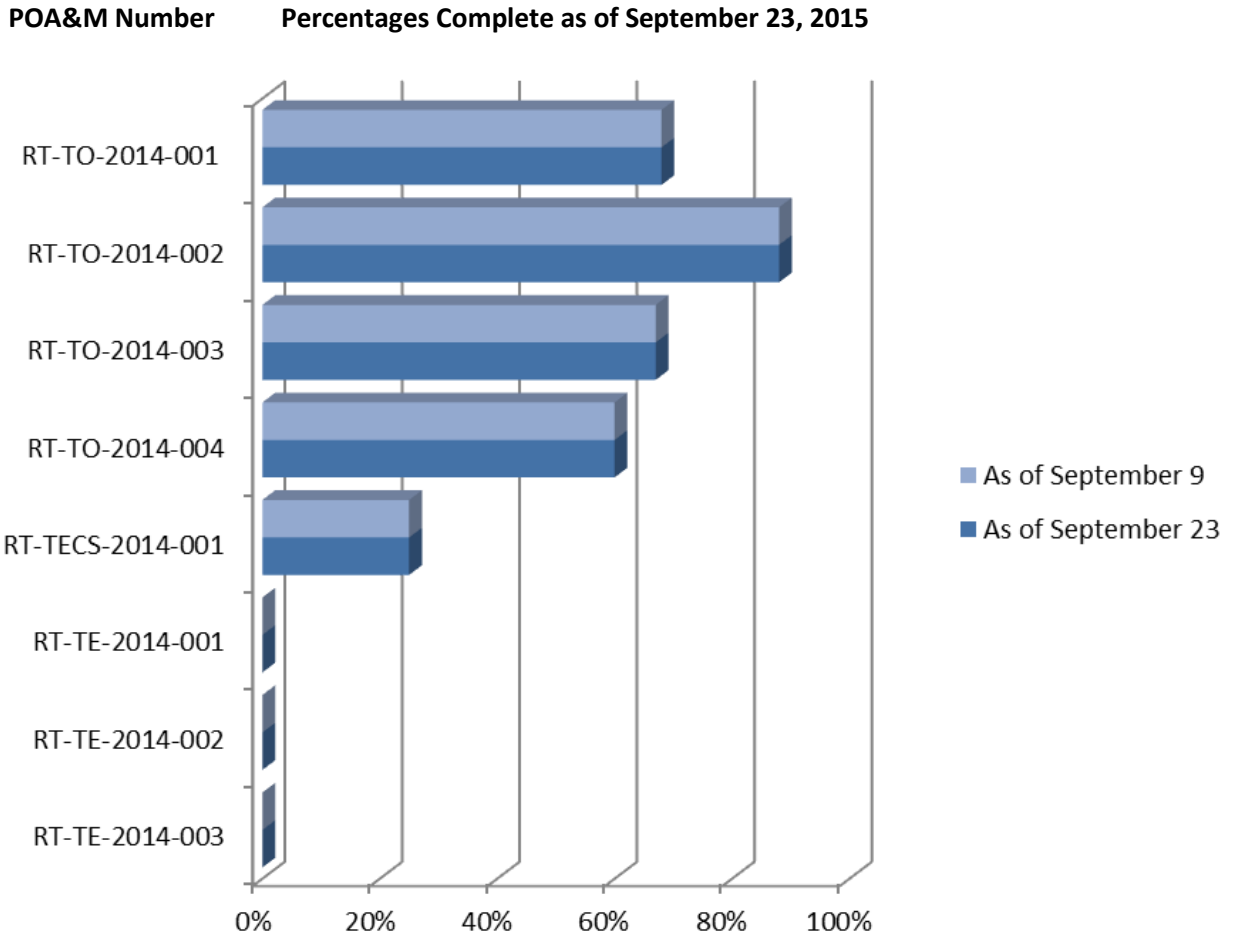
Evaluate and document domain trusts and FW rules between Grid Ops and IT Ops; Implement new FW rule configurations

(no progress since last report)

POA&M Percent Complete for Transmission

Mitigation Activities for Transmission, for TO, TEC, and TC combined, have not progressed for one month.

The percentage complete remain at 39% Complete



POA&M Details for Transmission

Each POA&M or finding from the original Security Assessment Report (SAR) consists of one or more tasks. Some tasks within a particular POAM may be progressing on schedule; others may be complete, while still others may have slipped past the initial estimated completion dates.

POA&M	Remediation Tasks	Progress Updates	Team
RT-TO-2014-001	<p>Work Completed: Configure Splunk to receive FIN data; Configure Splunk to receive all CNN network device logs where capable</p> <p>Work in Progress: Configure Tripwire to monitor root and system files on all DMZ systems capable of Tripwire (due, Sept 30, 2015.)</p>	(no progress for one month)	Andy McDonald, John Mare
RT-TO-2014-002	<p>Work Completed: Evaluate DGOZ GOPs to ensure only privileged roles can run executable files; The vendor (LANDESK) team was on site. Progress was made on scoping the HIPS solution</p> <p>Work in Progress: Investigate and scope Host-based Intrusion Prevention System (HIPS) solutions (due Sept 30, 2015.)</p>	(no progress for one month)	Andy McDonald, John Mare
RT-TO-2014-003	<p>Work Completed: Implement OU GPO for service accounts to enforce 16 character passwords (Requires coordination with numerous resource managers) <i>Note: Could only be enforced procedurally;</i> Create and enforce Control Center issue-specific password policy; Password length and complexity issue are incorporated into the BITA</p>	(no progress for one month)	Andy McDonald, John Mare, Rustin Jones

Work in Progress:

Update Windows Account Management Plan to reflect change in standard (due Dec 31, 2015.)

- 16 character service account passwords
- 12 character interactive user account passwords

Work not Started:

Establish tool and process to periodically test AD account's password strength and complexity in and isolated environment (due Dec 31, 2015)

RT-TO-2014-004

Work in Progress:

Remove the domain trust from BUD to DGOZ (due June 30, 2016 - *Note: Relying on CIP to provide solution*); Design and implement DMZ architecture that does not require the BUD trust (due June 30, 2015 - *Note: Competing strategies being worked out*); Review the necessity of all ports and services (i.e. RDP, Telnet, etc.) that transgress the DMZ boundary (due Dec 31, 2015 - *Note: Relying CIP to provide solution*); Progress was made on resolving competing strategies between the Control Center and Corporate IT

(no progress for one month)

Andy McDonald, John Mare

RT-TECS-2014-001
(Scott Lissit)

Work Completed:

Purchase and test secure USBs for use on SPC equipment

Work not Started:

Enable security on all FIN connected GE D-400s; Replace SEL-2020s, SEL-2030s, PRTUs and IP-Servers on the FIN with relays connected with secure GE D-400s; Replace all software One Time Password (OTP) tokens with hardware OTP tokens; all work is due to be completed within 12 months of approved funding date.

(no progress for one month)

RT-TE-2014-001 (unknown)	Work not Started: Configure files integrity tool (Tripwire) appropriately; Centralized logging of file integrity activity (Splunk) (both tasks due 1/30/15)	(no progress for one month)
RT-TE-2014-002 (unknown)	Work not Started: Update the system security (SSP) with authorization boundary and inventory (due 12/31/2014)	(no progress for one month)
RT-TE-2014-003 (unknown)	Work not Started: Integrate access control for SPC users and devices into the OMET plan; Implement monitoring for SPC devices to log unsuccessful access attempts. Add to the OMET plan (due 4/1/2016)	(no progress for one month)

Glossary

- **Application Control Database** – contains application signatures to check against, allowing the identification and control of applications on networks and endpoints regardless of port, protocol, and IP address used
- **AppLocker** – A feature in Windows 7 and Windows Server 2008 R2 that allows specification of which users or groups can run particular applications based on unique identities of files. Rules will allow or deny applications from running.
- **Domain Trusts** - Authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain).
- **End Point Protection** – A methodology for protecting a network by focusing on network devices (endpoints) by monitoring their status, activities, software, authorization and authentication. End Point Protection solutions are typically installed on any endpoint device, as well as network servers. Such software may include antivirus, antispyware, firewall and a host intrusion prevention system (HIPS).
- **File Integrity Monitoring** - an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.
- **Forefront** – A discontinued family of line-of-business security software by Microsoft Corporation. Several Forefront products were designed to help protect computer networks, network servers (such as Microsoft

Exchange Server and Microsoft SharePoint Server) and individual devices. As of 2015, the only actively developed Forefront product is Forefront Identity Manager which is designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system.

- **lan.bat** - a file that will load your driver and other files you wish to load while booting
- **LDAP** - Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet
- **Network Intrusion Detection System** - a system that tries to detect malicious activity by monitoring network traffic
- **Sophos** - A developer and vendor of computer security software and hardware, providing communication endpoint, encryption, network security, email security and mobile security as well as Unified Threat Management products.
- **Splunk (and Splunk Enterprise Security)** - A next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics and correlations. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.
- **Web Application Firewall** - An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.
- **Whitelisting** - A computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.