Department of Energy
Washington, DC 20585

July 29, 2021

Kartikay Mehrotra
Bloomberg News
Pier 3, Suite 201
San Francisco, CA 94111

Via email: kmehrotra2@bloomberg.net

RE: HQ-2020-00394-F

Dear Mr. Mehrotra:

This is a final response letter to the request for information that you sent to the Department of Energy (DOE) under the Freedom of Information Act (FOIA), 5 U.S.C. § 552. You requested:

> "I request access to and copies of the Bonnevile Red Team Report published between October 2014 and April 2015 ("the Records"). This request is ongoing, seeking copies of (or access to) all Records as they are filed with the Department of Energy. I am further requesting that the Records be provided to me on computer files or, if not maintained on computer files, in the same format as they are currently maintained at the Department of Energy."

On January 16, 2020, your request was transferred to DOE's Bonneville Power Administration (BPA) to conduct a search of its files and provide you with a response. Upon further review, BPA determined that they did not have jurisdiction and transferred your request back to DOE Headquarters. Your request was then assigned to DOE's Office of Enterprise Assessments (EA) to conduct a search of its files for responsive documents. EA began its search on March 11, 2020, which is the cut-off date for responsive documents. EA completed its search but did not locate any documents responsive to your request.

In an August 5, 2020, telephone call with me, Alexander C. Morris, confirmed via email with Ms. Kathy Ludunge, formerly of my office, you agreed to amend your request to extend the timeframe out 6 months to October, 2015.

Your amended request was assigned to DOE's Office of Enterprise Assessments (EA) to conduct a search of its files for responsive documents. EA began its search on August 10, 2020, which is the cut-off date for responsive documents. EA has completed its search and identified one (1) document responsive to your amended request. The document is being released to you as described in the accompanying index.

Upon review, DOE has determined that certain information contained within the documents should be withheld pursuant to Exemptions 5, 6 and 7(E) of the FOIA, 5 U.S.C. § 552, (b)(5), (b)(6) and (b)(7)(E).

Exemption 5 protects from mandatory disclosure "inter-agency or intra-agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency…." Exemption 5 incorporates the deliberative process privilege which protects recommendations, advice, and opinions that are part of the process by which agency decisions and polices are formulated. The information withheld under Exemption 5 consists of inter-agency pre-decisional information.

The withheld portions of the documents in question are pre-decisional and deliberative. The information is both pre-decisional, because it was developed before the agency adopted a final policy, and deliberative, in that it reflects the opinions of individuals who were consulted as part of the decision-making process. DOE may consider these preliminary views as part of the process that will lead to the agency's final policy decision about these matters. The documents and discussions do not represent a final agency position, and their release would compromise the deliberative process by which the government makes its decisions. Thus, portions of the documents are being withheld under Exemption 5 of the FOIA as pre-decisional material that is part of the agency's deliberative process.

With respect to the discretionary disclosure of deliberative information, the quality of agency decisions would be adversely affected if frank, written discussion of policy matters were inhibited by the knowledge that the content of such discussion might be made public. For this reason, DOE has determined that discretionary disclosure of the deliberative material is not in the public interest because foreseeable harm could result from such disclosure.

Exemption 6 is generally referred to as the "personal privacy" exemption; it provides that the disclosure requirements of FOIA do not apply to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" 5 U.S.C. § 552(b)(6). In applying Exemption 6, the DOE considered: 1) whether a significant privacy interest would be invaded; 2) whether the release of the information would further the public interest by shedding light on the operations or activities of the Government; and 3) whether in balancing the privacy interests against the public interest, disclosure would constitute a clearly unwarranted invasion of privacy.

The information withheld under Exemption 6 consists of a picture of DOE cybersecurity personnel. This information qualifies as "similar files" because it is information in which an individual has a privacy interest. Moreover, releasing the information could subject the individuals to unwarranted or unsolicited communications. Since no public interest would be served by disclosing this information, and since there is a viable privacy interest that would be threatened by such disclosure, Exemption 6 authorizes withholding the information. Therefore, we have determined that the public interest in the information's release does not outweigh the overriding privacy interests in keeping it

confidential.

Exemption 7 protects from disclosure "records or information compiled for law enforcement purposes" that fall within the purview of one or more of six enumerated categories. 5 U.S.C. § 552(b)(7). To qualify under Exemption 7, the information must have been compiled, either originally or at some later date, for a law enforcement purpose, which includes crime prevention and security measures, even if that is only one of the many purposes for compilation.

Exemption 7(E) provides that, "records or information compiled for law enforcement purposes" may be withheld from disclosure, but only to the extent that the production of such documents "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

The information withheld under Exemption 7(E) consists of DOE's cybersecurity and physical security investigative techniques and procedures. That information was compiled for preventative law enforcement and/or security purposes to prevent future illegal acts in the form of cyber security intrusions. Because the redacted portions of the enclosed documents contain information about DOE's investigative techniques that could be used by an individual to obtain classified or sensitive information on DOE networks without authorization, we are withholding this information pursuant to Exemption 7(E).

This satisfies the standard set forth at 5 U.S.C. § 552(a)(8)(A) that agencies shall withhold information under FOIA "only if (I) the agency reasonably foresees that disclosure would harm an interest protected by an exemption…; or (II) disclosure is prohibited by law…" 5 U.S.C. § 552(a)(8)(A) also provides that whenever full disclosure of a record is not possible, agencies shall "consider whether partial disclosure of information is possible…and (II) take reasonable steps necessary to segregate and release nonexempt information." Therefore, we have determined that, in certain instances, a partial disclosure is proper.

Pursuant to 10 C.F.R. § 1004.7(b)(2), I am the individual responsible for the determination to withhold the information described above. The FOIA requires that "any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt." 5 U.S.C. § 552(b). As a result, a redacted version of the documents is being released to you in accordance with 10 C.F.R. §1004.7(b)(3).

This decision, as well as 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 (this is the preferred method by the Office of Hearings and Appeals). 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 DOE's FOIA Public Liaison, Alexander Morris, FOIA Officer, Office of Public Information, at 202-586-5955, or by mail at MA-46/Forrestal Building 1000 Independence Avenue, S.W., Washington, D.C., 20585, 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 at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

The FOIA provides for the assessment of fees for the processing of requests. *See* 5 U.S.C. § 552(a)(4)(A)(i); *see also* 10 C.F.R. § 1004.9(a). In our June 23, 2020, letter you were informed that your request was placed in the "news media" category for fee purposes. Requesters in this category are charged fees for duplication only and are provided 100 pages at no cost. DOE's processing costs did not exceed $15.00, the minimum amount at which DOE assesses fees. Thus, no fees will be charged for processing your request.

This is a final response for DOE. If you have any questions about the processing of the request or this letter, you may contact Mr. William Mond, or me, at:

MA-46/ Forrestal Building
1000 Independence Avenue, S.W.
Washington, D.C. 20585
(202) 586-5955.

I appreciate the opportunity to assist you with this matter.

Sincerely,

ALEXANDER R MORRIS
Digitally signed by ALEXANDER MORRIS
Date: 2021.07.29 11:51:59 -04'00'

Alexander C. Morris
FOIA Officer
Office of Public Information

Enclosures

INDEX

Request #: HQ-2020-00394-F

Final response to amended request from Mr. Kartikay Mehrotra for:

> **"I request access to and copies of the Bonnevile Red Team Report published between October 2014 and April 2015 ("the Records"). This request is ongoing, seeking copies of (or access to) all Records as they are filed with the Department of Energy. I am further requesting that the Records be provided to me on computer files or, if not maintained on computer files, in the same format as they are currently maintained at the Department of Energy."**

In an August 5, 2020, telephone call with me, Alexander C. Morris, confirmed via email with Ms. Kathy Ludunge, formerly of my office, you agreed to amend your request to extend the timeframe out 6 months to October, 2015.

DOE's Office of Enterprise Assessments has completed its search and has located one (1) document responsive to your request.

- One (1) document *is being released in part pursuant to Exemptions 5, 6 and 7(E).*

Unannounced Independent Cyber Security Assessment at the

Bonneville Power Administration

~~OFFICIAL USE ONLY~~

~~May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: 7 Law Enforcement~~

~~Department of Energy review required before public release~~

~~Name/Org: William F. West/EA-21~~ ~~Date: July 1, 2015~~

~~Guidance (if applicable) CG-SS-4~~

July 2015

Office of Cyber and Security Assessments
Office of Enterprise Assessments
U.S. Department of Energy

DOES NOT CONTAIN
OFFICIAL USE ONLY INFORMATION

Name/Org: ACM / MA-46 Date: 6/9/2021

EA Enterprise Assessments

Table of Contents

Abbreviations Used in this Report

BPA	*Bonneville Power Administration*
BUD	*Bonneville User Domain*
DEV	*Development Network*
EA	*Office of Enterprise Assessments*
GTS	*General Transmission Support*
IDS	*Intrusion Detection System*
TCP	*Transmission Control Protocol*

This page intentionally left blank.

Executive Summary

At the request of the Bonneville Power Administration (BPA), the U.S. Department of Energy Office of Cyber and Security Assessments, within the Office of Enterprise Assessments (EA), performed an unannounced cyber security (Red Team) assessment of network security at BPA in Portland, Oregon, from April 17, 2014, to November 13, 2014. Red Team assessments differ from traditional network assessment activities in that they focus on identifying and exploiting the path of least resistance, rather than the full range of vulnerabilities that may exist within a network. Red Team assessments present a more accurate picture of a network's ability to withstand an attack from a real adversary because these assessments closely mirror the tools and techniques employed by nation-state adversaries.

BPA markets wholesale electrical power from several hydro projects in the Columbia River Basin, as well as a nuclear power plant and other smaller power plants. BPA operates and maintains approximately 75 percent of the high-voltage transmission in Idaho, Oregon, Washington, western Montana, and small parts of eastern Montana, California, Nevada, Utah, and Wyoming. This Red Team assessment was performed with the knowledge of the BPA Chief Operating Officer and Chief Information Security Officer. The assessment modeled the insider threat, as well as that posed by an outsider gaining limited physical access to BPA Headquarters. The approach included physically installing rogue devices on the network, performing automated vulnerability scans of the network, gathering network information and user account authentication credentials, assessing system vulnerabilities, and using identified vulnerabilities to install unauthorized software to garner additional authentication credentials to migrate to other systems on the network. These activities, by extension, assessed BPA's intrusion detection system and incident response capabilities. EA staff validated the assessment team's findings with BPA cyber security personnel, and conducted an outbrief with BPA senior management on December 8, 2014.

During the initial phase of this assessment, the EA assessment team gained physical access to the BPA Headquarters building on two separate occasions by circumventing normal procedures for visitors. On each occasion, EA connected a concealed computer to BPA's network. The concealed computers obtained an Internet Protocol address and joined BPA's network without requiring authentication or authorization. This attack tactic allowed the assessment team to gather information about the network and use it to further exploit the network. For approximately one month, the assessment team actively scanned, probed, and compromised several systems on BPA's network domains. The assessment team progressed from an unauthorized visitor gaining access to the BPA building, to simple access to BPA's internal network in the development domain, to being capable of exercising full control of both BPA's user domain and a domain run by a group referred to as critical business systems, which contains servers used for power marketing. With this level of control, the assessment team had access to servers

and information regarding BPA's operations, (b) (7)(E) , which controls the physical security systems and access points protecting the building.

The assessment team's level of access required only basic skills for creating rogue network devices, performing scanning, and harvesting credentials. No elaborate resources or highly sophisticated tools were needed. Contributing factors that allowed the assessment team to migrate across BPA's network included misconfiguration of a system, use of simple passwords, and shared or duplicated passwords across domains on multiple systems. Further, BPA's intrusion detection and incident response capabilities were found to be insufficient. EA assessment team activities generated a large amount of "noise" on the network, as well as specific activities, or events, on the network that could have been detected by automated systems and recorded in security logs. However, BPA did not detect the unauthorized computers connected to its network, the large amount of network traffic, or events such as multiple successful and unsuccessful login attempts. Effective intrusion detection and incident response capabilities would have detected these activities and alerted security personnel to the activity. (b) (7)(E) In the current state, it is very unlikely that BPA would detect a sophisticated, stealthy attacker on its network.

1 Introduction

The U.S. Department of Energy Office of Cyber and Security Assessments, within the Office of Enterprise Assessments (EA), performed an unannounced (Red Team) assessment at the Bonneville Power Administration (BPA) from April 17, 2014, to November 13, 2014. BPA markets wholesale electrical power from 31 Federal hydro projects in the Columbia River Basin, as well as a nuclear power plant and other smaller power plants. BPA operates and maintains approximately 75 percent of the high-voltage transmission in Idaho, Oregon, Washington, western Montana, and small parts of eastern Montana, California, Nevada, Utah, and Wyoming. This red team assessment was performed with the knowledge of the BPA Chief Operating Officer and Chief Information Security Officer. The primary purpose of this assessment was to attempt to evaluate BPA's ability to detect and deter an effort to gain access to BPA systems that could be manipulated to disrupt power delivery or BPA business operations. The following sections describe the methodology and tactics that were used, a timeline of events, results and analysis by topic area, and conclusions.

This page intentionally left blank.

2 Red Team Methodology and Tactics

The eventual methods that the EA assessment team used to gain a foothold in the BPA network were chosen to emulate a realistic attack vector that a malicious insider or an external adversary with unauthorized access might use. The tactics focused on issues that an adversary could leverage, including placement of rogue network devices on the internal network and using those network devices to migrate to other portions of the BPA network. The conduct of the assessment was described in a formal review plan approved in April 2014 by representatives of the "white cell" composed of the trusted agent, EA, the Joint Cybersecurity Coordination Center, the National Nuclear Security Administration Information Assurance Response Center, the Office of the Inspector General, and BPA.

This Red Team assessment evaluated certain aspects of BPA's cyber security program, including physical access to BPA's office areas, staff interaction with the assessors while entering buildings, installation of rogue devices (i.e., computers) onto BPA's network, and BPA's log correlation and detection of suspicious activities.

The tactics that the EA assessment team used were not based on a specific attack vector; instead, the assessment team followed the path of least resistance. Only basic measures were taken to avoid detection. The first tactic involved deploying a concealed computer (Figures 1 and 2) on two separate occasions to gain access to the network and perform exploratory scans of the BPA network.

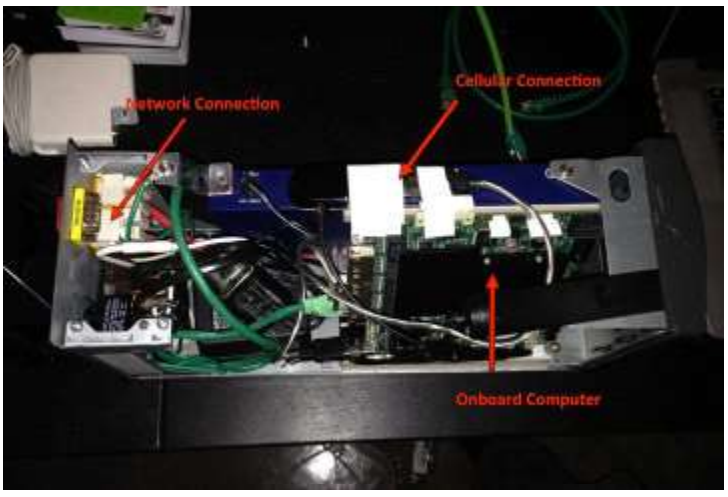

Figure 1. Concealed Computer Internal Components

The second tactic used a remote management console, also known as a management interface, on a compromised server to install a (b) (7)(E) (b) (7)(E) that allowed the EA assessment team access to the server's file system and the ability to execute command line utilities. The third tactic leveraged credentials acquired by the assessment team on one domain to gain access to other systems on another domain on the BPA network.

Figure 2. Concealed Computer with Shell

3 Chronology of Events

The chronology below details events and actions that the EA assessment team took while at BPA, as well as actions taken by site personnel, as observed by the assessment team. Analysis of these activities is provided in Section 4, Results and Analysis.

September 4, 2014

The assessment team entered BPA Headquarters in Portland, Oregon, (b) (7)(E) at approximately 4:15 p.m. (b) (7)(E)

(b) (7)(E)

.

The assessment team proceeded (b) (7)(E), waited in an unoccupied conference room until 5:00 p.m., and then deployed a computer concealed inside a power strip under a desk in a cubicle in the northeast corner of the building. This computer was configured with a cellular modem that allowed the assessment team to access BPA's network from a remote location via an encrypted tunnel.

September 5-11, 2014

The assessment team performed passive discovery of the BPA network, followed by active scans of discovered computers, to identify devices on the network and potential targets for compromise.

September 12-17, 2014

The assessment team noticed that its concealed computer appeared to be disconnected from the network, but the encrypted tunnel remained active. On September 17, the computer ceased to function entirely. The team later determined that the computer was disconnected and discarded when the conventional desk surface in the cubicle was replaced with a standing desk. No alerts or inquiries were generated by BPA personnel at this time.

October 17, 2014

The assessment team returned to Portland and entered BPA Headquarters through the route used previously. The assessment team proceeded to (b) (7)(E) and deployed a second covert computer (Figure 3). This second computer was concealed in a small uninterruptable power supply device, along with cellular telephone and computer networking devices, which the team connected to a network printer.

Figure 3. EA Assessment Team Member Deploying Concealed Computer

October 18-30, 2014

The assessment team performed slow exploratory scans of BPA's networks and attempted to identify populated network subnets.

October 30 – November 2, 2014

At the request of the trusted agent, the assessment team paused all activities while BPA investigated an unrelated security incident. The assessment team resumed when BPA determined that the incident was unrelated to EA's assessment.

November 3, 2014

The assessment team began to perform rapid internet control message protocol scans (used to identify computers that are on the network and receiving input) of BPA's networks. These scans were followed by further scans of discovered hosts for transmission control protocol (TCP) ports commonly associated with web application servers (e.g., Apache Tomcat) and server management interfaces. The assessment team examined each discovered service and performed manual probes for configuration errors and vulnerabilities.

November 4, 2014

The assessment team found an (b) (7)(E) in the development (DEV) domain that had no password configured on the management interface. The DEV domain is part of the network that BPA has designated for the installation and use of development computers. Using this interface, the assessment team installed a (b) (7)(E) that gave access to the server's file system and the ability to execute command line utilities.

November 6, 2014

The assessment team extracted the hashed password for the local (b) (7)(E) account from the compromised (b) (7)(E) This password hash was cracked in less than 30 seconds using commercially purchased hardware and software freely available on the Internet.

November 7, 2014

The assessment team attempted to log into all systems in the DEV domain (b) (7)(E) and found that 37 other systems in that domain were using the same password. The assessment team logged into each of these systems using the Windows remote desktop protocol and searched for information that could be used to access other systems on the BPA network. This led to the discovery of the (b) (7)(E) Windows Domains. GTS (or General Transmission Support) is BPA's critical business systems domain and contains servers that are used for power marketing functions. BUD (or Bonneville User Domain) is BPA's business network.

November 9, 2014

The assessment team (b) (7)(E) on each compromised system in the DEV domain. This tool intercepts and logs the unencrypted password for any account that authenticates to the compromised system. The tool immediately captured the credentials associated with a service account used to monitor and maintain systems in the DEV domain. The assessment team used these credentials to compromise the service account and install (b) (7)(E) DEV systems.

November 10, 2014

The assessment team gathered the credential logs from each compromised DEV system after regular business hours. The logs included 36 unique user names in the DEV domain. These user names were compared to the list of users in the (b) (7)(E) domain. The assessment team then attempted to log into (b) (7)(E) systems using the passwords from matching DEV accounts. Several (b) (7)(E) accounts, including one server administrator, were accessible using the same passwords. The assessment team used this administrator account to access and install the (b) (7)(E) on 13 additional servers in the (b) (7)(E) domain.

November 11, 2014

The assessment team captured the credentials associated with a high-level administrator account in the (b) (7)(E) domain. This password was used to access and compromise six terminal servers used by network administrators. The assessment team also gained access to the VMware VSphere console used to manage the entire GTS virtual server infrastructure. This infrastructure included the Production servers, the Alternate Data Center, the Integrated Test Environment, and the GTS "demilitarized" zone.

November 12, 2014

The assessment team identified a password for an account in the DEV domain that included the word (b) (7)(E) There was a matching account in the (b) (7)(E) domain, so the assessment team changed (b) (7)(E) to (b) (7)(E) in the password and used it to successfully log into a server in the (b) (7)(E) domain. This account had administrative access to a server in the (b) (7)(E) domain. The user directories on these servers were searched and yielded information about BPA operations, including (b) (7)(E) , which controls the physical security systems (e.g., cameras, alarms, sensors) and access points (badge readers and gates for access to the building).

November 13, 2014

The assessment team explored the (b) (7)(E) domain and considered discovering paths into the (b) (7)(E) systems, the (b) (7)(E) , and the (b) (7)(E) that houses the supervisory control and data acquisition systems used by Transmission Services. Because of the significance of some of the identified vulnerabilities and the need to provide the details to BPA to facilitate corrective actions, EA concluded all BPA Red Team activities.

November 18, 2014

After the assessment team revealed its tactics and methodology, BPA identified and located the unauthorized computer after it failed and disabled a multi-function printer.

4 Results and Analysis

Information in this section was determined through the activities that the assessment team performed from September 4 to November 13, 2014.

Physical Intrusion Detection

(b) (7)(E)

Once inside the facility, the assessment team, on two separate occasions, was able to install unauthorized, concealed computers.

Network Intrusion Detection and Incident Response

The assessment team connected concealed non-BPA computers into BPA's network. Both concealed computers obtained an Internet Protocol address and communicated on the network without authentication or authorization. Each concealed computer remained undetected for the duration of the assessment team activities.

The assessment team scanned BPA's networks, generating a significant amount of network traffic. The initial scans were performed using stealth, but no attempt was made to obfuscate later scans. BPA did not detect these assessment team activities.(b) (7)(E)

In addition to scanning, the assessment team logged into compromised systems on BPA's DEV domain and installed software to intercept and log unencrypted account information. BPA did not detect or report these assessment team activities.

Vulnerability Scanning

The assessment team gained an initial foothold in BPA's Windows network through a misconfigured (b) (7)(E) (b) (7)(E)

System Configuration

BPA has standards and procedures for deploying production servers but did not follow those standards when the DEV domain was created. (b) (7)(E) In addition, servers were deployed without being properly configured or secured. These development servers were accessible from most BPA networks and could, in turn, access most BPA networks.

Password Reuse

(b) (7)(E)

Event Correlation and Intrusion Detection

The assessment team performed nearly all activities between 5 p.m. and 6 a.m. Pacific Standard Time.

(b) (7)(E) The following table demonstrates specific events and the evidence each would have generated. Proper correlation of these events might have caused BPA staff to investigate and respond to the anomalies.

EA Action	Evidence Available to BPA
(b) (7)(E)	(b) (7)(E)

*Media Access Control
**Dynamic Host Configuration Protocol

5 Conclusions

Although the assessment team's initial access was gained in September 2014, the subsequent loss of connectivity with the first rogue computer resulted in work not beginning in earnest until after the second rogue computer was deployed in October 2014. The assessment team actively scanned, probed, and compromised the BPA network for nearly a month. (b) (7)(E)

Extremely aggressive techniques were used, especially in the final week. These activities generated a massive quantity of "noise" on the BPA network, but at no point were any assessment team activities detected by BPA cyber security staff, system owners, users, or any other formal group within BPA.

The level of access that the assessment team acquired did not require the level of capability of a nation-state threat. The techniques used were not "cutting edge" or particularly stealthy. Despite these factors, BPA did not detect the assessment team on the network. (b) (5)

The security implications of this inspection for the BPA information systems and their support to the BPA mission are significant. The combination of physical security limitations and basic flaws in cyber defenses demonstrates a substantial risk of potential compromise and exploitation of important business and operational information systems by moderate and advanced cyber threats.

APPENDIX A
TEAM COMPOSITION

A.1 Management

Glenn S. Podonsky, Director, Office of Enterprise Assessments
William A. Eckroade, Deputy Director, Office of Enterprise Assessments
John S. Boulden III, Director, Office of Cyber and Security Assessments
William F. West, Director, Office of Cyber Assessments

A.2 Quality Review Board

William A. Eckroade
John S. Boulden III
Thomas C. Messer
Michael A. Kilpatrick
George E. Armstrong

A.3 Administrative Support

Heather Jeffrey

A.4 Assessment Team

Jeff Thomas (Team Lead)
Mike Petruzzi
Mike Guthrie
Mark Carey
Jeremy Dodson