



Deborah J. Jeffrey
Inspector General

August 12, 2016

MEMORANDUM

TO: Tom Hanley
Chief Information Officer

FROM: Deborah J. Jeffrey /s/
Inspector General

SUBJECT: Report on the Corporation for National and Community Service's Covered Systems under the 2015 Cybersecurity Act

Attached is the final report on CNCS's access control policies, procedures, and practices, as required by Section 406 of the Cybersecurity Act of 2015.

Based on the foregoing information, we conclude that CNCS's policies and practices for access controls appear to generally reflect Federal standards, though there remains opportunities to strengthen these protections. Additional information bearing on security measures discussed in this report will be addressed in our forthcoming 2016 FISMA evaluation report.

We appreciate the courtesies and assistance provided by you and your staff during the review. Should you have any questions about this report, please contact Guy Hadsall, Chief Technology Officer, at 202-606-9375.

Attachment

Cc: Asim Mishra, Chief of Staff
Jeremy Joseph, General Counsel
Jeffrey Page, Chief Operating Officer
Stacy Dawn, Chief Information Security Officer

**Office of Inspector General
Corporation for National and
Community Service**

**REPORT ON THE
CORPORATION FOR NATIONAL AND COMMUNITY
SERVICE'S COVERED SYSTEMS UNDER THE 2015
CYBERSECURITY ACT**

Office of Inspector General

Corporation for
**NATIONAL &
COMMUNITY
SERVICE** 

Prepared by:

Office of Inspector General
Corporation for National & Community
Service

Summary of Results

The Cybersecurity Act of 2015, Sec 406 requires Inspectors General of agencies with covered systems¹ to submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report on agency policies, practices, and controls related to logical access and security management. The statute also calls for a determination whether the logical access policies and practices meet appropriate standards.

The Office of Inspector General for the Corporation for National and Community Service (CNCS-OIG) has completed this work based in part on our Federal Information Security Modernization Act (FISMA) evaluation for 2015 and in conjunction with the FISMA evaluation in progress for 2016, together with information provided by Corporation for National and Community Service (CNCS or the Corporation) personnel. Except as stated in the FISMA evaluation reports, we did not verify or test the effectiveness of the access controls that CNCS has implemented to protect its systems and applications from unauthorized users.

Based on the foregoing information, we conclude that CNCS's policies and practices for logical access controls generally reflect Federal standards, subject to certain limitations described herein. Additional information bearing on security measures will be addressed in our forthcoming 2016 FISMA evaluation report.

Background

The Corporation defines Personally Identified Information (PII) as “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.” That definition follows the definition in Office of Management and Budget Circular M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* and the standards found in National Institute of Standards and Technology, Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*.

The following systems at CNCS contain PII:²

Electronic System for Programs, Agreements & National service participants (eSPAN)

eSPAN is the central database for maintaining CNCS application and grant data and AmeriCorps program and member data, including member-related payment data.

¹ Covered systems include systems that provide access to personally identifiable information (PII), such as name, social security number, address, or biometric information.

² Privacy Impact Assessment (PIA) are published for all CNCS systems that have PII. <http://www.nationalservice.gov/site-policy-and-notices/privacy-policy>

The eGrants component manages the Corporation-wide grant process from the application stage to grant closeout. On average, CNCS receives approximately 7000 applications and manages 2700 active grants each year.

The AmeriCorps Member Portal (Member Portal) is a self-service, online system for member management, including recruitment, enrollment, service (including service hours performed), close of service, education award balance, and post-service matters. In addition, the Member Portal provides CNCS and project sponsors with a consistent interface for gathering necessary data from and about members and applicants.

General Support System

The CNCS General Support System (GSS) provides general automated data processing and support for CNCS and the general public using CNCS information technology (IT) resources. Network services include security support, as well as mobile device management and Voice Over Internet Protocol (VoIP) telephone service. The GSS hosts or provides connectivity for major applications (MAs), including eSPAN and the Momentum Enterprise Solution (Momentum). It also supports minor applications, such as office automation, human capital, travel, and Freedom of Information Act (FOIA) and Privacy Act requests.

Momentum Enterprise Solution

The Momentum is the core CNCS electronic financial management system, by which CNCS records, processes and reports financial transactions. CNCS considers Momentum to be a major application.

AmeriCorps Volunteers in Service to America Health Benefits System

The AmeriCorps Volunteers in Service to America Program (VISTA) provides its members certain health benefits, requiring PII to manage the benefits of individual members. Access to the VISTA Health Benefits System is restricted to VISTA members and the vendor, International Medical Group (IMG).

AmeriCorps Childcare Benefit System

The AmeriCorps Childcare Benefit System (ACBS) consolidates information relating to the management of childcare benefits available to qualified, full-time participants in national service programs administered by CNCS. Benefits are paid directly to the qualified childcare providers. PII is necessary to administer each member's benefits.

NCCC Health Benefits System

The National Civilian Community Corps (NCCC) National Health Benefit System (NHBS) manages the healthcare benefits plan available to all NCCC and FEMA Corps members. These benefits are automatic upon entry into training or service. This plan is not insurance, but rather a basic health benefit package. The electronic system maintains the member PII needed for management of each individual's benefits.

Information Pursuant to the Cybersecurity Act of 2015

- a. A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.***

CNCS has logical access policies³ which are documented in its Cybersecurity Policy, System Security Plans and associated CNCS Cybersecurity Control Families document, as well as in its privacy policies. Additionally, the Corporation has policies and practices specifically addressing data retention and privacy. These policies are posted on the CNCS internal website.

The logical access policies are implemented through the following systems procedures and practices:

- Privacy Policy
- On Boarding and Off Boarding Employees and Contractors System
- CNCS Cybersecurity User Training
- CNCS Cybersecurity Rules of Behavior
- General Support System standard operating procedures for managing Active Directory object controls
- System Security Plans (SSP) for enhanced logical access controls for each covered system.

Our 2015 FISMA evaluation found that CNCS was in the midst of rebuilding its information security program. Serious vulnerabilities remained from prior years, and CNCS-OIG discovered a new weakness in access controls. Since the publication of the evaluation report in November 2015, CNCS-OIG has monitored efforts to strengthen information security, and we have noted improvements. We expect to report in the forthcoming 2016 FISMA evaluation that CNCS has resolved the access control weakness and has generally strengthened its Cybersecurity Program.

Since last year, CNCS has reviewed its system and enterprise security controls, has identified additional opportunities to improve cybersecurity and has issued new and revised information technology policies. The Office of Information Technology (OIT) has standardized the documentation for system security across all CNCS systems, to achieve enterprise-wide consistency. OIT continues to prepare for the Department of Homeland Security (DHS) Continuous Diagnostics and Monitoring (CDM) implementation this fall, which should further enhance the Corporation's logical access control, network visibility, and incident response.

Based on the information that the Corporation provided, we conclude that its policies and practices for logical access to covered systems generally reflect appropriate standards, though there remain opportunities to strengthen these protections. We did

³ In information technology, logical access controls are tools and protocols for granting or denying specific requests to obtain or use information and related information processing services.

not verify or test the effectiveness of CNCS's access controls in preventing incursions by unauthorized users.

b. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

CNCS does not require multi-factor authentication⁴ for privileged users.⁵ Access for such privileged users is governed by the SSP and the General Support System SSP for administering Active Directory⁶ users and groups. CNCS has provided limited training for privileged users as a group, but has not conducted specific role-based training, as recommended by CNCS-OIG in prior FISMA evaluations.

General access controls include requiring that privileged users perform their network administrative functions through a separate account with a unique password and that they undergo annual privileged-user security training. In addition, privileged users must comply with the routine security measures that govern access by non-privileged users, such as strong passwords that must be changed every 60 days, user lockout after five unsuccessful logon attempts, and automated mechanisms to disable and remove inactive accounts after 30 days.

c. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

CNCS asserts that it is not required to implement multi-factor authentication in conformity with Homeland Security Presidential Directive 12: *Policy for a Common Identify Standard for Federal employees and Contractors (HSPD-12)*, <https://www.dhs.gov/homeland-security-presidential-directive-12>, because it is a government corporation and is considered a micro agency. In 2005, the Office of Management and Budget (OMB) exempted CNCS from the requirement to adopt multi-factor authentication on the grounds that it is a government corporation. OMB Memo M-05-24; Attachment A, Question 1A. In connection with the 2015 FISMA evaluation, the Chief Information Officer (CIO) stated that CNCS would begin a phased implementation of two-factor authentication in the form of Personal Identity Verification (PIV)⁷ cards for privileged users in FY 2017, assuming that the appropriation included sufficient funding.

⁴ The term "multi-factor authentication" means the use of not fewer than two authentication factors, such as the following: (A) Information known only to the user, such as a password or personal identification number; (B) An access device that is provided to the user, such as a cryptographic identification device or token; (C) A unique biometric characteristic of the user. Cybersecurity Act of 2015, Sec 406 (a) Definitions, 4 Multi-factor Authentication

⁵ The term "privileged user" means a user who has access to system control, monitoring, or administrative functions. Cybersecurity Act of 2015, Sec 406 (a) Definitions, (5) Privileged user

⁶ Active Directory is a service running on most Windows servers that authenticates and authorizes users and computers in a Windows network.

⁷ A personal identity verification (PIV) card is a United States Federal smart card that contains the necessary data for the cardholder to be granted to Federal facilities and information systems and assure appropriate levels of security for all applicable Federal applications. The criteria for PIV cards was established by Federal Information Processing Standard (FIPS) FIPS 201, which was formally entitled Personal Identity Verification of Federal Employees and Contractors. FIPS 201 was

CNCS considers the use of shared digital certificates on its laptops for remote access to be a form of multi-factor authentication. Another form of multi-factor authentication, according to CNCS, is the requirement that users authenticate prior to startup of their laptop/desktop operating system (*i.e.*, pre-boot whole disk encryption). Both forms of user authentication are on the computer, which by definition is not multi-factor authentication. As reported in the FY 2014⁸ and FY 2015⁹ FISMA evaluation reports, CNCS-OIG disagrees with characterizing these measures as multi-factor authentication, because they are not independent of the computer.

d. A description of the following information security management practices used by the covered agency regarding the covered system:

i. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

CNCS has adopted configuration management policies and procedures that require the inventory of software on its covered systems, with documentation by CNCS and by its vendor. Changes to CNCS systems, including the addition or removal of software, require approval by the Corporation's Technical Control Board (TCB) and Program Change Control Board (PCCB), which document the approved changes.

CSRA, Inc., the vendor, provides hardware and software management services and owns the software. It maintains inventories through manufacturer and serial number data in purchasing databases, receiving documents, and tracking spreadsheets and its procedures call for updating of the system inventory prior to installation of new components. In addition, CSRA, Inc. identifies, probes and collects software and system data by means of the following enterprise software tools:

- Microsoft Definitive Media Library
- LANDesk—automatically updates the inventory upon addition of a laptop or desktop to CNCS's Active Directory domain
- RemedyForce—maintains the inventory for CNCS devices and identifies the user to whom a device has been issued
- Maas360—validates the inventory for smart phones issued to CNCS personnel
- SolarWinds—validates the inventory for network devices and servers.

developed to satisfy the requirements of HSPD 12, which requires a common identification standard for all Federal employees and contractors. FIPS 201, which is intended to be a living document, specifies the interface and data elements of the PIV card, the technical acquisition and formatting requirements for biometric data on the card and acceptable cryptographic algorithms and key sizes.

⁸ FY14 IG FISMA Report https://www.cncsoig.gov/sites/default/files/15-03_0.pdf

⁹ FY15 IG FISMA Report <https://www.cncsoig.gov/sites/default/files/16-03.pdf>

ii. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

CNCS has advised CNCS-OIG that its contractor CSRA, Inc., procures, manages and decommissions its laptops/desktops centrally, using Active Directory¹⁰ and other enterprise software tools to build, deploy, manage and administer to a known standard configuration. Users cannot install software applications on their laptops and/or desktop computers. The standard laptops and/or desktop configuration includes a defined set of software applications to include software agents that support the central management of software licensing.

CNCS manages software licenses centrally through CSRA, Inc. Should a user be approved to have non-standard software, the contractor procures/assigns and pushes it out to the user's laptop/desktop from a central configuration management repository. The contractor periodically inventories software on the laptops and desktops and reconciles discrepancies with the Corporation.

iii. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats including:

- Data Loss Prevention Capabilities

CNCS has very limited ability to monitor or detect exfiltration of sensitive data, including PII. [REDACTED]

In recognition that there may be legitimate needs to share PII and other sensitive information outside CNCS network boundaries, CNCS provides users with a secure channel for communicating PII through authenticated Federal Information Processing Standards (FIPS)¹¹-compliant encrypted (e.g., MoveIT DMZ) file transfer. [REDACTED]

CNCS has implemented USB drive encryption (i.e., Microsoft BitLocker) by default on all laptops and desktops to better protect agency information. Upon insertion of a USB drive into a CNCS laptop and/or desktop, the operating system asks the user if s/he

¹⁰ Active Directory is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services

¹¹ The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to accredit cryptographic modules. The title is Security Requirements for Cryptographic Modules.

agrees to encryption of the USB drive; if the user agrees, then the system encrypts the drive and allows the data transfer. If the user does not agree, data transfer will not occur. All data moved from the Corporation's laptop and/or desktop to a USB drive is required to be encrypted.

Efforts to monitor or detect exfiltration of sensitive data are hindered by the fact that CNCS systems contain a large quantity of stale PII, for which no current user is responsible and for which CNCS has no inventory. Although this material is not currently in use, it has remained accessible by many CNCS staff members, creating an unnecessary risk. OIT advises that it has taken measures to limit access to the data and to develop a plan to account for PII by owner and appropriately control or dispose of it.

- *Forensics and Visibility Capabilities*

CNCS's digital forensic capabilities consist of intrusion detection systems, antivirus/malware applications, web-filtering applications and firewalls. DHS provides limited capability to collect and analyze data entering and exiting its Internet boundary through the Trusted Internet Connection (TIC) program. The CIO has advised that, should CNCS require digital computer forensic assistance, it would seek the support from DHS.

In FY 2015, the Corporation signed a Memorandum of Understanding (MOU) with DHS National Cybersecurity Assessments and Technical Services (NCATS) to participate in the monthly Federal Cyber Exposure Scorecard program. The NCATS scans the Corporation's public facing systems for vulnerabilities, with a monthly report on vulnerabilities, according to their severity. CNCS has also entered into an MOU to participate in DHS's Continuous Diagnostics and Mitigation program and is preparing for the implementation in FY 2017. With the implementation of CDM, the Corporation expects to have increased visibility into its network traffic.

- *Digital Rights Management Capabilities*

CNCS does not have the capability to support digital rights management (DRM) of individual user files, although subsystems within the network offer limited visibility into potential protected application and server software. Users are permitted to copy and/or download data files, to include music and video, onto their laptops and/or desktops. By policy and practice, access controls do not allow non-privileged users to install software on laptops/desktops or on servers.

CNCS has outsourced its software license management to CSRA, Inc. To support its configuration management, the vendor uses the Microsoft Definitive Media Library to administer CNCS-approved software deployments. Software to be deployed on servers and laptops/desktops must be approved by the Corporation's Technical Review Board (TRB) using a documented change management process.

Additionally, the Corporation is in the midst of a multi-year project to deploy Microsoft SharePoint for enterprise content management. Under this project, files and folders

from the current shared directories on internal file servers are being migrated to SharePoint sites.

iv. A description of how the covered agency is using the capabilities described in (ii)

CNCS reports that it, together with its contractor CSRA, Inc., routinely monitors the CNCS network for intrusions, malicious software, access control violations, and attacks against its network. According to OIT, when the contractor receives an alert, it follows CNCS policy for incident response. The CIO stated that the Corporation regularly reviews the reports from DHS NCATS regarding vulnerabilities found in the public-facing systems, and responds according to its Cybersecurity policy and practices.

CSRA, Inc. routinely uses the Microsoft software license management solution to manage the Corporation's laptop/desktop and server software licenses. Based upon the approval of the TRB, software is installed, updated, or removed.

The Corporation began a multi-year project to migrate user files to an enterprise content management system, which provides limited DRM capabilities. These capabilities include increased access control of files, accounting of file ownership, improved records management, and logging of user accesses. CNCS does not yet have an automated common repository of system and access logs, which can be monitored and mined for anomalies and irregularities. OIT reports that it has an ongoing project to implement such a capability.

v. If the covered agency is not utilizing capabilities described in (ii), a description of the reasons for not utilizing such capabilities.

In general, CNCS is using the limited capabilities currently at its disposal and working to develop others. The CIO appears to appreciate the need to enhance IT security and is working actively to improve the defense, detection and response to threats against covered systems. CNCS-OIG looks forward to the future implementation of important safeguards.

e. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (d)

The Corporation's Cybersecurity Policy on its face applies to all CNCS data and systems that store and process government data, including contractor systems. CNCS policy requires that anyone, including contractor staff, who requests access to CNCS internal networks and systems must undergo appropriate training and submit a signed Rules of Behavior acknowledgment prior to obtaining user access. The basic training includes user security awareness and privacy modules. Privileged users (e.g., network and systems administrators) are required to have additional security training.

CNCS-OIG has not verified whether vendors in fact comply with these requirements, or whether CNCS monitors their compliance.

CNCS Acquisition Policy 350, requires that specific IT security and privacy requirements must be included in all CNCS contracts based on the particular nature of the IT services and the information/data requirements of the contract. It is up to the CNCS Contracting Officer's Representative to identify the specific security needs and ensure the necessary contract clauses are in the contract and ensure the vendor implements them properly.

Appendix A: Objectives, Scope, and Methodology

Section 406 of the Cybersecurity Act of 2015 requires Inspectors General for agencies with covered systems to report to Congress specific information regarding the agencies logical access policies and security management practice. The Act's definition of a covered system includes federal computer systems that provide access to personally identifiable information (PII). Since the Corporation has such systems, we conducted this inspection to identify and provide the requested information.

In keeping with the requirements of the Cybersecurity Act of 2015, this review was undertaken in order to:

- Identify and document Corporation logical access policies and practices
- Identify and document Corporation logical access controls and multi-factor authentication
- Identify and document Corporation information security management practices
- Identify and document Corporation policies and procedures to ensure that service providers are implementing information security management practices.

This review included Corporation logical access policies, practices and controls for CNCS covered systems that provide access to PII. We did not verify or test the effectiveness of these controls or other security management measures.