
Information about specific vulnerabilities in IT systems has been redacted from the publicly released version of this report. The information withheld was compiled in connection with OIG law enforcement responsibilities and consists of information that, if released publicly, could lead to the circumvention of the law.

EXPORT-IMPORT BANK
***of the* UNITED STATES**
INSPECTOR GENERAL

Memorandum

To: Appropriate committees of jurisdiction in the Senate and the House of Representatives

From: Terry Settle TLS
Assistant Inspector General for Audits

Subject: Results of the Cybersecurity Information Sharing Act, Section 406 Data Call

Date: August 12, 2016

This memorandum presents our response to Title IV of the Cybersecurity Information Sharing Act of 2015, section 406, *Federal Computer Security*. The Cybersecurity Information Sharing Act of 2015 (CISA) is a U.S. federal law designed to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes". The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. Section 406 of the Act entitled *Federal Computer Security* required Agency Inspectors General, no later than 240 days after its enactment, to submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include the following information regarding the Federal computer systems of the covered agency:

> (A) A description of the logical access standards used by the covered agency to access a covered system.
>
> (B) A description of the logical access controls used by the covered agency to govern access to covered systems by privileged users.
>
> (C) If the covered agency does not use logical access controls or multi-factor logical access controls to access a covered system, a description of the reasons for not using such controls.
>
> (D) A description of the following data security management practices used.

(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.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) Data loss prevention capabilities;
(II) Forensic and visibility capabilities; or
(III) Digital rights management capabilities.

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

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

(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 data security management practices described in subparagraph (D).

Our office engaged the independent public accounting firm of Cotton & Company (Cotton) to perform the data call in response to CISA. These services included performing a review of the Bank's computer systems that are classified as national security systems[1], or that provide access to personally identifiable information (PII). Cotton gathered all the necessary information to adequately respond to the topics in section 406, *Federal Computer Security,* through interviews with the Office of the Chief Information Officer (OCIO) personnel and review of Ex-Im Bank's policies, procedures, practices and controls over logical access, data security management, and contractor security for all of the Bank's systems that provide access to PII. Cotton leveraged previous FY2015 Federal Information Security Modernization Act (FISMA) audit work. For areas that required more detailed information to appropriately address the CISA topics, Cotton performed additional information gathering and review activities. The data call was performed as a non-audit service from March 2016 to May 2016; therefore, this memorandum only summarizes the results of the data call.

[1] United States Code Title 40, Section 11103 describes a national security system as a telecommunications or information system operated by the federal government, the function, operation, or use of which—
(A) Involves intelligence activities;
(B) Involves cryptologic activities related to national security;
(C) Involves command and control of military forces;
(D) Involves equipment that is an integral part of a weapon or weapons system; or
(E) Subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.
(2) Limitation.—
Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

RESULTS

Cotton reviewed the Bank's computer systems and determined that the Bank does not operate any national security systems, but it does operate systems that provide access to PII. These systems, also referred to as "covered systems" included in this CISA data call are as follows:

- Infrastructure General Support System (GSS)
- Oracle GSS
- Ex-Im Online
- Financial Management System-Next Generation (FMS-NG)
- Office 365
- System Center Service Manager (SCSM)
- Ex-Im Badge System
- Inspired eLearning
- Application Processing System (APS)
- Moodys
- ERS/Hyperion
- Comprizon Suite

The summarized results of the data call for the topics of section 406, *Federal Computer Security* are presented in the Attachment*, Export-Import Bank CISA Data Call Response*. Cotton determined that the information provided by EXIM Bank was complete and fully addressed the requirements of section 406. However, Cotton did not evaluate whether appropriate standards were followed as part of this data call. An assessment of whether appropriate standards were followed will be provided as part of the annual FISMA report and Cyberscope responses during the FY2016 FISMA audit.

The CISA data call was not an audit and therefore, was not conducted in accordance with generally accepted government auditing standards. All the information gathered in response to the topics in section 406, *Federal Computer Security* was sufficient to provide a reasonable basis for the summary results. The observations were discussed with management officials on June 22, 2016, and their comments were included where appropriate.

If you have any questions, please contact me at (202) 565-3498 or terry.settle@exim.gov. You can obtain additional information about the Export-Import Bank Office of Inspector General and the Inspector General Act of 1978 at www.exim.gov/oig.

Attachment

cc:

Fred Hochberg, Chairman and President
Angela Freyre, General Counsel
C.J. Hall, Executive Vice President and Chief Operating Officer
Howard Spira, Chief Information Officer
John Lowry, Director, Information Technology Security and Systems Assurance
Inci Tonguch-Murray, Deputy Chief Financial Officer
Cristopolis Dieguez, Business Compliance Analyst
George Bills, Partner, Cotton & Company LLP

ATTACHMENT

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)