Office of the Inspector General
U.S. Department of Justice

Report on the Department of Justice's Cybersecurity Logical Access Controls and Data Security Management Practices Pursuant to the Cybersecurity Act of 2015, Section 406, Federal Computer Security

Audit Division 16-23

August 2016

REPORT ON THE DEPARTMENT OF JUSTICE'S CYBERSECURITY LOGICAL ACCESS CONTROLS AND DATA SECURITY MANAGEMENT PRACTICES PURSUANT TO THE CYBERSECURITY ACT OF 2015, SECTION 406, FEDERAL COMPUTER SECURITY

OFFICE OF THE INSPECTOR GENERAL COMMENTARY AND SUMMARY

The Cybersecurity Act of 2015 § 406 (Section 406) requires the Department of Justice (DOJ) Office of the Inspector General (OIG) to submit a report to Congress on DOJ's cybersecurity policies, procedures, practices, and capabilities for national security systems and systems that provide access to personally identifiable information. The OIG contracted with KPMG LLP (KPMG) to perform a review and prepare this report pursuant to the Section 406 reporting requirement.

KPMG's approach to accomplishing the Section 406 reporting requirement was to collect information regarding the design of DOJ's information technology cybersecurity practices. KPMG interviewed DOJ management and inspected DOJ policies and practices. KPMG also leveraged applicable system information from the fiscal year (FY) 2016 Federal Information Security Modernization Act (FISMA) audit and previous OIG FISMA audit reports for the following cybersecurity areas applicable to Section 406:

- Logical Access Policies and Procedures
- Logical Access and Multi-Factor Authentication for Privileged Users
- Data Security Management Practices
- Data Security Management Practices over Contractors

Summary of Results

KPMG found that DOJ has developed policies and procedures to implement the controls addressed in Section 406 to establish an information security program compliant with the National Institute of Standards and Technology.

For Logical Access Policies and Multi-factor Authentication, KPMG found that DOJ is making progress in implementing personal identity verification (PIV) logical access for privileged and unprivileged users across the organization, but significant work still needs to occur related to the PIV multi-factor implementation. DOJ management told KPMG that for unclassified systems, currently the PIV multi-factor authentication implementation is at 60 percent for privileged users and 58 percent for unprivileged users. This is primarily due to an Intelligence Community Component starting its PIV implementation at the beginning of FY 2016. KPMG noted that DOJ created a corrective active plan to satisfy the OMB requirement for 100 percent PIV implementation for privileged users. DOJ management indicated that the PIV implementation projected completion date is September 30, 2016, for privileged users and is September 30, 2017, for unprivileged users. Finally, for those network and application accounts that are not yet able to accept PIV authentication, Secure ID tokens and usernames with strong passwords are still used for multi-factor authentication.

In the area of Data Security Management Practices, DOJ is currently utilizing Secure Socket Layer and user activity monitoring tools for forensics and visibility capability. KPMG obtained evidence and observed that the tools were operating as asserted by DOJ management. DOJ management stated that the required tools are all deployed across DOJ; however more coordination needs to occur at the component level to fully deploy all of the tools to all of the components.

Lastly, in terms of Data Security Management Practices over Contractors, DOJ released the Procurement Guidance Document (PGD) 15-03, *Security of Information and Information Systems*, requiring mandatory security clauses be included in DOJ procurement documents.

The results of this review were presented to DOJ management prior to the issuance of the report. DOJ management concurred with the contents of the report.

Report on the Department of Justice's Cybersecurity Logical Access Controls and Data Security Management Practices Pursuant to The Cybersecurity Act of 2015, Section 406, Federal Computer Security, Pub. L. 114-113.

Prepared for: U.S. Department of Justice (DOJ)
Office of the Inspector General

As of July 13, 2016

KPMG LLP
1676 International Drive
Mclean, VA 22102

TABLE OF CONTENTS

KPMG

KPMG LLP
1676 International Drive
McLean, VA 22102

Inspector General
U.S. Department of Justice

This report presents the results of our work conducted to address The Cybersecurity Act of 2015, Section 406, Federal Computer Security, Pub. L. 114-113 (Section 406) requirements. This report and the work therein was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. Our work was performed during the period of July 1, 2016 through July 13, 2016.

On December 18, 2015, the President of the United States signed the Consolidated Appropriations Act, 2016. This Act included Section 406, which focuses on the current cybersecurity logical access controls and data security management monitoring controls. Congress requires Inspectors General to submit a report on select security controls identified in Section 406 for national security systems and systems that provide access to personally identifiable information (PII).

Our objectives were to report on the Department of Justice's (DOJ) cybersecurity logical access controls, multi-factor authentication, privileged users' access, data security management practices, and data security management practices over contractors related to covered national security systems and systems that provide access to PII. KPMG LLP (KPMG) interviewed DOJ management and inspected DOJ policies and practices. KPMG also leveraged information from the fiscal year 2016 Federal Information Security Modernization Act (FISMA) audit and previous DOJ Office of the Inspector General (OIG) component and system level FISMA audit reports.

KPMG found that DOJ has developed policies and procedures to implement the controls addressed in Section 406 to establish an information security program compliant with the National Institute of Standards and Technology. In addition, KPMG found that DOJ is making progress in implementing personal identity verification (PIV) logical access for all privileged and unprivileged users across the organization; however significant work still needs to occur on the PIV implementation for network and application accounts. For those network and application accounts that are not yet able to accept PIV, SecureID tokens and username with strong passwords are used for multi-factor authentication.

KPMG LLP

BACKGROUND

On December 18, 2015, the President of the United States signed the Consolidated Appropriations Act, 2016. This Act included The Cybersecurity Act of 2015, Section 406, Federal Computer Security (Section 406), which requires agencies with a national security system or a federal computer system that provides access to personally identifiable information (PII) (covered systems) to describe cybersecurity logical access controls, multi-factor authentication, privileged users' access, and information security management practices related to the covered systems.

Congress requires agency Inspectors General to submit a report on selected security controls identified in Section 406, which are discussed in the Results section of this report, to the appropriate committees of jurisdiction in the Senate and the House of Representatives.[1]

OBJECTIVES, SCOPE AND METHODOLOGY

Our objectives were to report on the Department of Justice's (DOJ) cybersecurity logical access controls, multi-factor authentication, privileged users' access, data security management practices, and data security management practices over contractors related to covered national security systems and systems that provide access to PII. This report and the work therein was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. The work was performed at DOJ facilities located in Washington, DC during the period of July 1, 2016 through July 13, 2016.

KPMG LLP's (KPMG) approach to accomplishing the Section 406 reporting requirement was to collect information regarding the design of DOJ's information technology (IT) cybersecurity practices. The design of DOJ's security controls refers to DOJ cybersecurity-related and other DOJ security policies and guidelines. KPMG reviewed pertinent security and system documentation related to the design and implementation of access controls, including DOJ information security policies, procedures, and practices. KPMG also interviewed DOJ security managers and other individuals with cybersecurity IT responsibilities. In addition, KPMG leveraged information obtained during the fiscal year 2016 Federal Information Security Modernization Act (FISMA) audit, as well as other DOJ Office of the Inspector General (OIG) reports related the cybersecurity areas described in Section 406.

As part of the fiscal year 2016 FISMA audit, KPMG, in concurrence with the OIG, selected a representative subset of DOJ information systems and security controls to test and assess DOJ's progress towards implementing minimum security standards and requirements commensurate with each system's security categorization and risk. KPMG used the results of these system reviews to describe DOJ's cybersecurity practices and prepare the Section 406 report.

[1] Under Public Law 114-113, the Inspector General of each covered agency (an agency that operates a covered system) is directed to submit to the appropriate committees of jurisdiction in the Senate and House of Representatives, not later than 240 days after the enactment of the Act, a report which shall include information collected from the covered agency for selected logical security controls.

RESULTS

KPMG interviewed DOJ management and performed limited observations related to the following cybersecurity areas:

- Logical Access Policies and Procedures
- Logical Access and Multi-Factor Authentication for Privileged Users
- Data Security Management Practices
- Data Security Management Practices over Contractors

Logical Access Policies and Procedures

Describe the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.[2]

DOJ utilizes the following logical access policies and procedures to access covered systems entity-wide:

- DOJ Order 2640.2F, *Information Technology Security*
- DOJ Information Technology Security Standards
- US DOJ Cybersecurity Program Management Plan Fiscal Year 2016
- DOJ Strong Authentication Plan
- Security Public Key Infrastructure (PKI) Implementation Memo
- Memorandum of Understanding between DOJ and Defense Information Systems Agency (DISA)

KPMG obtained and inspected the DOJ Order 2640.2F (Order), *Information Technology Security*, which establishes the uniform policy, responsibilities and authorities for the protection of IT systems that store, process or transmit DOJ information. The provisions of the Order include logical access policies and practices that apply to all government and contractor IT systems and users supporting the operations and assets of DOJ. To support the provisions of the Order, DOJ has implemented the DOJ Information Technology Security Standards (ITSS) that outline the minimum security control requirements for Federal Information Processing Standard Low, Moderate, and High impact systems that process, store, or transmit unclassified or classified information. The ITSS are derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 and Committee on National Security Systems (CNSS) Instruction 1253.

Unclassified System Requirements

DOJ management indicated that the DOJ personal identity verification (PIV) card is the logical access control and credentialing solution for the Identity Credential Access Management (ICAM) program for unclassified systems, and will continue to serve as the primary two-factor authentication token for logical access to DOJ systems. KPMG obtained and inspected the DOJ Strong Authentication Plan, released in May 2016, which provides all DOJ components

[2] Pub. L. No. 114-113, Sections 406(b)(2)(A) and (C) (2015).

with standard authentication requirements that will result in accelerated PIV implementation across DOJ. With the exception of the September 30, 2015 PIV requirement for privileged users accessing DOJ networks, some key points of the document, effective October 1, 2016, include the following requirements:

- Privileged users must use the PIV credential to authenticate for both network and application access;
- Unprivileged users who qualify to receive a PIV credential must use it for both network and application access;
- Unprivileged network users who do not qualify for a PIV credential must use an alternative Level of Assurance (LOA)-4 credential (PIV-I) for network access;
- Remote access to the network must utilize the PIV or PIV-I credential for authentication to the remote access solution;
- Remote access from government furnished equipment (GFE) must use a virtual private network (VPN) solution;
- Remote access from non-GFE must use a Virtual Desktop Interface;
- Non-GFE computers must be equipped with a PIV card reader that has been tested and approved by the Government Services Administration and has been procured in compliance with DOJ Procurement Guidance for supply chain risk management;
- Externally-accessible applications must be assessed using the DOJ E-Authentication Risk Assessment Template to determine the minimum Level of Assurance required for authentication; and
- Outlook Web Access (OWA) must require LOA-4 (PIV or PIV-I) credentials for authentication; therefore, OWA is not authorized if LOA-4 cannot be achieved.

Additionally, Justice Management Division (JMD) management indicated that the DOJ ICAM program provides the core security services which establish verified identities linked to trusted credentials providing proper levels of access. DOJ’s ICAM is the critical integration and management of digital identities, credentials, attributes, and access control into a comprehensive enterprise services approach. DOJ’s ICAM program supports the President’s Cybersecurity National Action Plan (CNAP). DOJ’s ICAM program identifies the priorities driving the strategic initiatives and related project efforts, as well as the intermediate steps and performance measures required to realize the key benefits of a unified DOJ ICAM program.

Additional Classified System Requirements

DOJ management indicated they comply with Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, which establishes requirements for the protection of all classified networks and systems, as well as the secure sharing of classified information by authorized users. DOJ has fully implemented CNSS Directive No. 506, *National Directive to Implementation Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks*, mandating the use of token-based public key infrastructure (PKI) across all DOJ Secret enclaves. DOJ leverages Defense Information System Agency (DISA) for the Secret Public Key Infrastructure (SPKI) services. An intelligence community component currently maintains and owns the PKI infrastructure and Certificate Authority for its Secret networks but is working with CNSS on testing and implementation with migrating to the DISA system. This transition is currently scheduled for completion in FY 2017.

Logical Access and Multi-Factor Authentication for Privileged Users

Describe and list the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users. If the covered agency does not use logical access controls or multi-factor authentication to access controls or multi-factor authentication used by the covered agency to govern access to covered system, describe the reasons for not using such logical access controls or multi-factor authentication.[3]

The primary multi-factor authentication used to govern access to covered systems by privileged users is the PIV credential. The use of the PIV credential for logical access to the network is mandatory for all privileged users, and is primarily enforced through machine-based registry settings updated via group policy settings. This credential can be further utilized by covered systems via three methods.

- DOJ Federation Services – DOJ Federation Services extends the network PIV credential authentication to the covered systems via a Federated single sign-on session.
- Direct PIV Credential enablement – Covered systems can alternatively be modified to directly authenticate the PIV credential via code or configuration changes.
- Privileged Access Management (PAM) tool – For covered systems which do not utilize Active Directory for directory services or authentication, and cannot be enabled directly to authenticate the PIV credential, an authentication proxy can be used to require PIV authentication for privileged users. A PAM is a specialized authentication proxy for privileged users. All privileged access to the covered system must go through the PAM, which requires PIV authentication. The user can "check out" a privileged user account credential and conduct their required duties, all of which is auditable to that specific user. DOJ is working with the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation program to examine potential PAM tools.

KPMG inspected the Assistant Attorney General for Administration memorandum, Strengthening Information Technology Systems - Mandatory Strong Authentication for Privilege Users and found that it states, "As part of an effort to strengthen government information systems, the Office of Management and Budget (OMB) identified on June 11, 2015 several actions requiring accelerated completion to prevent and detect cyber intrusions. In particular, I am asking for your help in meeting a fast approaching deadline for two-factor authentication for all privileged user access. This will ensure our system administrators and those with the most extensive access rights enter and manage our networks, systems, and data with their identities both verified and corroborated. One-factor authentication, i.e. username with password combination alone, is an acute vulnerability and must be corrected. If your component is unable to implement two-factor authentication for privileged users by June 30, 2015, those privileged accounts must be disabled on that date."

KPMG found that DOJ is making progress in implementing PIV logical access for privileged accounts across the organization; however significant work still needs to occur on the PIV implementation for network and application accounts. For those network and application

[3] Pub. L. No. 114-113, Sections 406(b)(2)(B) and (C) (2015).

accounts that are not yet able to accept PIV, Secure ID tokens for multi-factor authentication and username and strong passwords are still in use.

DOJ management indicated that for unclassified systems, currently the PIV multi-factor authentication is at 60 percent for privileged users and 58 percent for unprivileged users.[4] This is primarily due to an Intelligence Community Component starting its PIV multi-factor implementation at the beginning of FY 2016. KPMG noted that DOJ created a corrective active plan to satisfy the OMB requirement for 100 percent PIV implementation for privileged users. DOJ management indicated that the PIV implementation projected completion date is September 30, 2016, for privileged users and is September 30, 2017, for unprivileged users. DOJ management further indicated that the multi-factor authentication for all users on the classified side is at 100 percent for both secret and top secret environments.

Data Security Management Practices

Inventories

Describe 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. [5]

DOJ utilizes its inventory management solutions, which allow DOJ to establish a holistic view of the network inventory. This data is fed into a custom-developed Endpoint Lifecycle Management System (ELMS), which consolidates and presents understandable data to users. Continuous monitoring is performed through a variety of tools with the results compiled regularly via the Security Posture Dashboard Report (SPDR). The ELMS data is synthesized into SDPR, which allows a quick and concise view of the inventory, its configuration, and vulnerabilities for each DOJ Component. Components are able to use this data for a multitude of tasks, including the tracking of software licenses, configuration, and vulnerability remediation.

The DOJ Configuration Management Plan is applicable to all DOJ IT systems, unclassified and classified, including systems that are DOJ-owned but operated by contractors and systems that are outside of DOJ control, such as cloud systems, that collect, store, process, or transmit DOJ information. As a minimum standard for secure configuration management, DOJ components are required to the below requirements, but not limited to:

- Establish and maintain baseline configuration inventories of information systems, including hardware, software, firmware, and documentation.
- Establish a configuration change control process to ensure proposed changes are evaluated, tested, properly approved, and documented before being put into production.
- Establish and document mandatory configuration settings for information technology products employed within the information system.

[4] OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, released on October 30, 2015, no longer included provisions for exceptions to the PIV mandate, such as removing new hires, temporary employees, and lost or damaged PIV cards. As a result, these types of users are now included in the current PIV implementation count.

[5] Pub. L. No. 114-113, Section 406(b)(2)(D)(i) (2015).

- Identify, document, and approve deviations from the mandatory configuration settings based on operational requirements and security impact analysis.
- Ensure vendor-supplied system software is still supported by the vendor.
- Identify, report, and correct information system flaws and promptly install security-relevant software updates.

DOJ software licenses are managed in accordance with the license agreements and DOJ's procurement requirements. Procurement Guidance Document (PGD) 16-02, *Acquisition of IT Equipment, Software, and/or Services*, describes the processes and procedures that DOJ must follow when acquiring, by contract, order, reimbursable agreement, or otherwise, covered IT equipment, software, and/or services, to ensure compliance with Federal Information Technology Acquisition Reform Act and OMB's guidance.

Monitoring Capabilities

Describe the capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including: (I) data loss prevention capabilities; (II) forensics and visibility capabilities or (III) digital rights management capabilities. Describe how the covered agency is using the capabilities described in clause (ii).[6]

The Justice Security Operations Center (JSOC) provides continuous situational awareness and defense-in-depth monitoring and detection at all layers of DOJ's network. The table below details DOJ's cybersecurity tools that support the prevention/monitoring and detection of cybersecurity threats. DOJ has participated in the DHS Continuous Diagnostics and Mitigation program and has capable tools to address data loss, visibility, forensics, and inventory. DOJ management indicated that they are currently utilizing Secure Socket Layer (SSL) monitoring and User Activity Monitoring tools for forensics and visibility capability.

[6] Pub. L. No. 114-113, Section 406(b)(2)(D)(ii) and (iii) (2015).

Tools	Description	Scope	Value Proposition
Data Loss Prevention – Web	The Data Loss Prevention (DLP) – Web solution detects and prevents the loss of sensitive data via websites through increased network visibility, context, and speed required to identify advanced threats. The project deploys a DOJ-wide capability that will identify active attackers on the network and block data theft.	The DLP-Web tool detects personally identifiable information (PII) leaving the network and the tools and tactics of advanced attackers, including advanced malware, exploits, command and control activity, and data theft techniques bypassing traditional network security systems (e.g., firewalls, intrusion prevention systems). It encompasses web-based services throughout DOJ.	This defense-in-depth model assists DOJ-level and component-level efforts to detect adversaries at every stage of the attack lifecycle. [100 percent compliant across all components]
Endpoint Exploit Prevention	This solution hardens and prevents vulnerabilities from being exploited on endpoints. The capabilities will make targets more difficult to exploit.	The endpoint exploit prevention tool configures certain operating systems and applications for resiliency against mechanisms that could potentially compromise the software.	The software adds an additional layer of application defense to prevent the exploitation of vulnerabilities. [90 percent compliant across all components]
Network Activity Logging and Analysis	This solution provides the capability to perform expanded logging and analysis capacity across networks (application logs, database logs, network logs, configuration files, and performance data). This capability will enable more effective detection of anomalous network activity and improved attack forensics performance.	The logging and analysis tool incorporates a platform for the collection and searching of machine data (e.g., audit logs). This is deployed across the networks, but will have no impact at endpoint user level; subsequent post-attack analysis will impact primarily only the infected device.	The capability increases operational intelligence and provides deeper insight into machine data logs – resulting in greater detection of malicious activity within DOJ networks, and better post-attack forensics analysis. [25 percent compliant across all components]

Tools	Description	Scope	Value Proposition
Packet Capture and Cyber Analytics	This solution provides an advanced network-traffic analytics packet capture (PCAP) capability to increase the efficiency and effectiveness of cybersecurity analysis and incident response. The capability allows rapid detection, assessment, and containment of data breaches and provides deep network visibility and analysis quickly. The PCAP technology records live data streams for future forensic analysis.	The PCAP tool provides comprehensive, near real-time analysis of network-traffic for rapid threat response and minimizes the need to issue alerts to users. The tool will be used on the live data streams across DOJ.	This capability provides the ability for extended network PCAP up to 12 months to allow for deeper forensic analysis of incidents and detection of suspicious network behavior. [100 percent compliant. This tool is at the DOJ boundary and should not be installed at the component level]
Data Loss Prevention - Email	This solution allows DOJ to set policies that identify and categorize Social Security Number (SSN) data in automated policy-driven actions to block.	The *DLP* module will scan outbound emails for specific PII-related keywords (such as well-formed (SSN) and if detected, automatically stop the email from being transmitted. This will only affect email transmitted from an internal DOJ email address to an external non-DOJ email address.	This DLP solution will prevent accidental disclosures of PII to external untrusted entities. [100 percent compliant. This tool is at the DOJ boundary and should not be installed at the component level]
Secure Socket Layer (SSL) Visibility	This tool addresses and enforces acceptable use policies for inbound and outbound encrypted traffic, protect against advanced threats, and strengthen existing network security infrastructure; all while adhering to data privacy and compliance demands. The SSL Visibility Appliance helps to remove risks arising from lack of visibility into SSL traffic.	The *SSL Visibility* Appliance is an integral component to any enterprise SSL encrypted management strategy, by offering complete visibility into encrypted traffic without requiring the duplication of security appliances or re-architecting of network infrastructure.	This solution provides encrypted traffic management solution set to eliminate the encrypted traffic blind spot while preserving privacy, policy, compliance and the investment in the security infrastructure. [83 percent compliant across all components]

Tools	Description	Scope	Value Proposition
Malware Analysis	These appliances are integrated to auto-generate and share malware threat protection data to stop advanced targeted attacks across the web and email threat vectors and malware resident on file shares.	The malware analysis tool provides a secure environment to test, replay, characterize, and document advanced malicious activities; reveals attack lifecycles, from initial exploits and malware execution paths to callback destinations and download attempts.	This solution allows DOJ to better understand and evaluate malware attacks to better defend against them. [100 percent compliant. This tool is at the DOJ boundary and should not be installed at the component level]
User Activity Monitoring	These agents are installed onto user workstations to capture and monitor user activity for later review and analysis.	These agents perform user activity monitoring to track user actions, including file read/writes/changes, file movement, logins, etc.	This solution supports DOJ's Insider Threat Prevention and Detection Program and monitors all user activity on DOJ's networks. [100 percent compliant]

If the covered agency is not utilizing capabilities described in clause (ii), describe the reasons for not utilizing such capabilities.[7]

KPMG obtained evidence and observed the tools were operating as intended by DOJ management. However, DOJ management indicated that more coordination needs to occur at the component level to fully deploy all of the tools to all of the components.

Data Security Management Practices over Contractors

Describe 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.[8]

DOJ released PGD 15-03, *Security of Information and Information Systems,* requiring mandatory security clauses to be included in DOJ procurement documents. This guidance applies to any solicitation, whether written or oral, issued on or after the date of this guidance, that will result in a covered contract. A covered contract is any contract, order or other commitment under which the contractor, or a subcontractor at any tier, including a cloud service provider, may access, collect, store, process, maintain, use, share, retrieve, disseminate,

[7] Pub. L. No. 114-113, Section 406(b)(2)(D)(iv) (2015).

[8] Pub. L. No. 114-113, Section 406(b)(2)(E) (2015).

transmit, or dispose of DOJ Information. Covered contracts include, but are not limited to, service contracts (e.g., litigation and Freedom of Information Act support contracts in which the contractor scans documents containing DOJ Information and such information is collected, stored, processed, maintained, used, shared, retrieved, disseminated, transmitted, or disposed of using the contractor's Information System).

The *DOJ Security Assessment and Authorization Handbook* outlines the process, documentation requirements, and automated tools essential to performing the successful security assessment and authorization of DOJ information systems. Based on the NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and the Committee on National Security Systems Policy No. 22, Information Assurance Risk Management Policy for National Security Systems, the DOJ security assessment and authorization process has been designed to align with existing policy, standards, and guidance resulting in the assurance that security controls for DOJ IT systems are implemented and assessed in accordance with established DOJ security requirements.

The results of this review were presented to DOJ management prior to the issuance of the report. DOJ management concurred with the contents of the report.

Appendix 1

LIST OF ACRONYMS

Acronym	Definition
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CNAP	Cybersecurity National Action Plan
CNSS	Committee on National Security Systems
DHS	Department of Homeland Security
DISA	Defense Information System Agency
DLP	Data Loss Prevention
DOJ	U.S. Department of Justice
ELMS	Endpoint Lifecycle Management System
ICAM	Identity, Credential, and Access Management
FIPS	Federal Information Processing System
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GFE	Government Furnished Equipment
IT	Information Technology
ITSS	Information Technology Security Standard
JMD	Justice Management Division
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OWA	Outlook Web Access
PAM	Privileged Access Management
PCAP	Packet Capture
PKI	Public Key Infrastructure
PGD	Procurement Guidance Document
PII	Personal Identifiable Information
PIV	Personal Identity Verification
SP	Special Publication
SPDR	Security Posture Dashboard Report
SSL	Secure Socket Layer
SSN	Social Security Number

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig