

~~SECRET//NOFORN~~

Office of Inspector General of the Intelligence Community



Evaluation Report

(U) Fiscal Year 2012 Independent Evaluation of ODNI Compliance with the Federal Information Security Management Act of 2002

AUD-2012-008

21 November 2012

Important Notice

This report contains information that the Office of the Inspector General of the Intelligence Community has determined is confidential, sensitive, or protected by Federal Law, including protection from public disclosure under the Freedom of Information Act (FOIA) 5 USC § 552. Recipients may not further disseminate this information without the express permission of the Office of the Inspector General of the Intelligence Community personnel. Accordingly, the use, dissemination, distribution or reproduction of this information to or by unauthorized or unintended recipients may be unlawful. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative, civil, and/or criminal penalties. This report should be safeguarded to prevent improper disclosure at all times. Authorized recipients who receive requests to release this report should refer the requestor to the Office of the Inspector General of the Intelligence Community.

Classified By: (b)(3)
Derived From: ODNI INF S-12
Reason 1.4(g)
Declassify On: 20371001

~~SECRET//NOFORN~~

(U) TABLE OF CONTENTS

- I. (U) Executive Summary2**
- II. (U) Background4**
- III. (U) Objective, Scope, and Methodology5**
 - 1. (U) Objective 5
 - 2. (U) Scope and Methodology 5
 - 3. (U) FISMA Reporting Changes 6
- IV. (U) Evaluation Results7**
 - 1. (U) Continuous Monitoring Management..... 8
 - 2. (U) Security Configuration Management..... 9
 - 3. (U) Risk Management 12
 - 4. (U) Plan of Action and Milestones (POA&M)..... 14
 - 5. (U) Contingency Planning 16
 - 6. (U) Security Capital Planning..... 19
 - 7. (U) Systems Inventory..... 21
- V. (U) Follow-Up on Open Recommendations24**
- (U) Appendix A: Acronyms28**
- (U) Appendix B: FY 2012 IG FISMA Metrics Results29**
- (U) Appendix C: Management Comments40**

(U) LIST OF TABLES

- (U) Table 1: FY 2012 Systems Reviewed 13
- (U) Table 2: Summary of System Contingency Plans 18
- (U) Table 3: Systems Inventory Submission Summary 21
- (U) Table 4: FY 2009 FISMA Recommendations 24
- (U) Table 5: FY 2010 FISMA Recommendations 25
- (U) Table 6: FY 2011 FISMA Recommendations 26

~~SECRET//NOFORN~~

I. (U) Executive Summary

(U) The Federal Information Security Management Act of 2002 (FISMA) requires Federal agencies to establish security measures for information systems that support their operations and report annually on those measures.¹ FISMA also requires that an annual independent evaluation be performed by the agencies' Office of Inspector General (OIG) or by an independent external auditor.

~~(U//FOUO)~~ The objective of this evaluation was to provide an independent review of the Office of the Director of National Intelligence's (ODNI) information security program and practices as required by FISMA. Specifically, the purpose was to determine the adequacy of the information security programs for MSD and the Intelligence Community Chief Information Officer (IC CIO). Within ODNI, two groups are responsible for information systems: the Mission Support Division (MSD), which is responsible for internal ODNI systems, and the IC CIO Data Management Division, which is responsible for assisting the IC CIO with leading the IC in information assurance and information management governance to ensure a secure, robust, integrated Information Technology (IT) enterprise. To perform the evaluation, we applied the Department of Homeland Security's (DHS) Fiscal Year (FY) 2012 FISMA metrics, which cover 12 categories, and followed up on progress to address open recommendations from the FY 2009, FY 2010, and FY 2011 FISMA reports.

~~(U//FOUO)~~ Two metric categories, *Identity and Access Management* and *Security Training*, were not applicable to our evaluation because ODNI follows Central Intelligence Agency (CIA) processes and those metrics were reviewed during the CIA IG's evaluation. A third metric category, *Remote Access Management*, was not evaluated because ODNI did not have a remote access requirement in FY 2012. Of the remaining nine metric categories, *Incident Response and Reporting* and *Contractor Systems* had an established program that met the DHS program attribute requirements.

~~(U//FOUO)~~ Consequently, for the remaining 7 metric categories, we identified areas for improvement and produced 12 recommendations for ODNI information security programs. The seven metric categories were:

1. Continuous Monitoring Management
2. Security Configuration Management
3. Risk Management
4. Plan of Action and Milestones

¹ (U) Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et. seq.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

5. Contingency Planning
6. Security Capital Planning
7. Systems Inventory

(U//~~FOUO~~) We also assessed the ODNI's progress on addressing open recommendations from the FY 2009, FY 2010, and FY 2011 FISMA reports. Since July 2011, the ODNI closed 17 recommendations from the FISMA reports issued in FY 2009, FY 2010, and FY 2011. Those recommendations were designed to improve security controls testing and configuration management oversight. Additionally, we administratively closed two legacy recommendations from FY 2009 and FY 2010 since the same recommendation was included in this year's report. Also, in June 2011, the Intelligence Community Enterprise Collaboration Center (Intelink) Program transitioned from ODNI to the National Security Agency (NSA) per a memorandum of understanding between the IC CIO and the NSA CIO. Because of that transition, the IC IG sent the NSA IG the FY 2011 FISMA report that included all open recommendations for Intelink. The NSA OIG has reviewed the report and initiated an audit to determine if the prior deficiencies identified in the FY 2011 FISMA report were still present. Because the NSA OIG is now responsible for evaluating the adequacy of the Intelink information security program, the 32 open recommendations for Intelink were administratively closed for the ODNI.

(U//~~FOUO~~) In addition to this year's recommendations, two recommendations remain open from 2011 (See Table 6).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

II. (U) Background

(U) FISMA was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA compliance is a matter of national security and is scrutinized at the highest levels of Government.

(U) FISMA requires each agency to develop, document, and implement an agency-wide program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA requires heads of Federal agencies to provide information security protections, commensurate with the risk and magnitude of harm, from misuse or destruction of the agency's information or systems. FISMA recognizes the unique position of an agency CIO and asks each of them to implement FISMA provisions through agency information security officers. As the head of the IC, the DNI has delegated this authority to the IC CIO to ensure compliance with FISMA. The IC CIO is the senior official who heads the Office of the IC CIO.

(U) Independent Evaluations. FISMA requires an annual independent evaluation of the information security program and practices of an agency in order to determine its effectiveness.² For an agency with an OIG appointed under the Inspector General Act of 1978 or any other law, the evaluation is performed annually either by the OIG or by an independent external auditor, as determined by the OIG. For an agency operating or exercising control of a "national security system," as defined by FISMA, which includes ODNI, only an entity designated by the agency head may perform the independent evaluation.

² (U) 44 U.S.C. § 3545.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

III. (U) Objective, Scope, and Methodology

1. (U) Objective

(U//~~FOUO~~) The objective of this evaluation was to provide an independent review of the ODNI information security program and practices as required by FISMA. Specifically, the purpose of the evaluation was to determine the adequacy and status of the information security programs for the ODNI's internal operations. Additionally, we followed up on steps taken by management to address open recommendations made in the FY 2009, FY 2010, and FY 2011 FISMA reports.

2. (U) Scope and Methodology

(U) We performed this evaluation from April 2012 through July 2012, in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate documentation to provide a reasonable basis for our findings and conclusions based on the evaluation objectives. We evaluated the adequacy and effectiveness of the ODNI's information security programs in accordance with the DHS FY 2012 IG FISMA metrics.

(U//~~FOUO~~) We conducted interviews with officials and staff from MSD and the IC Information Assurance Directorate.³ We also interviewed officers from CIA's OIG and the Global Communications Service's Infrastructure Services Group (ISG).

(U//~~FOUO~~) To achieve our evaluation objective, we reviewed information and documentation provided to us by MSD, IC CIO, CIA OIG, and ISG officials. Information included internal policies and procedures; ODNI's internal systems inventories from MSD; risk management data for selected systems; system security test information; backup and recovery procedures; plan of action and milestones (POA&M) for systems; incident reporting; and security configuration management (CM) documentation.

³ (U//~~FOUO~~) The Intelligence Community Information Assurance Directorate assists the IC CIO with appropriate mechanisms for IA, Cyber Security, Information Security, Certification & Accreditation (C&A) Testing, Compliance Validation, and Risk Management to improve efficiencies and enhance information sharing across the IC, Federal Government, and allied partners.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

3. (U) FISMA Reporting Changes

(U) Changes to FISMA Requirements for FY 2009, FY 2010, and FY 2011.

In FY 2008, the Office of Management and Budget (OMB) initiated changes to improve both the FISMA reporting process and the use of metrics to increase the value of agency FISMA efforts. Beginning in FY 2009, OMB introduced its CyberSecurity Automated Repository and Management Application (CyberScope), which is an unclassified automated reporting tool. OMB then required Federal agencies, including the CIOs, OIGs, and Senior Agency Officials for Privacy, to obtain OMB's annual instructions and metrics from CyberScope. Agencies were also instructed to enter the results of their annual FISMA reviews in Cyberscope to enable OMB to directly upload the data. However, the IC was unable to use the application due to the classified nature of its FISMA information. Therefore, for FY 2009, FY 2010, and FY 2011, the IC OIGs provided their FISMA reports to OMB through classified channels. In June 2012, the IC CIO officials announced the availability of a classified IC CyberScope (ICCS) reporting application to streamline mandated FISMA reporting. The IC CIO conducted a short pilot from 20 June 2012 through 13 July 2012, which uncovered issues that are still undergoing review. Consequently, the IC will not use the ICCS for the FY 2012 FISMA reports.

(U) The OMB Memorandum 10-28, dated 6 July 2010, designated DHS with operational responsibilities for FISMA, which includes developing and finalizing the IG and CIO FISMA metrics.

(U) On 6 March 2012, DHS released the final FY 2012 IG FISMA metrics. Those metrics require that OIGs report on 12 categories:

1. Continuous Monitoring Management
2. Configuration Management
3. Identity and Access Management
4. Incident Response and Reporting
5. Risk Management
6. Security Training
7. Plan of Action and Milestones (POA&M)
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems
11. Security Capital Planning
12. Systems Inventory

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

IV. (U) Evaluation Results

~~(U//FOUO)~~ While both MSD and the IC CIO have made improvements to their information security initiatives that have addressed prior year OIG recommendations, we identified FISMA metric areas that require further improvement. This evaluation highlights FISMA program strengths and identifies information security areas within the ODNI that are not in compliance with FISMA criteria.

~~(U//FOUO)~~ The programs that met DHS FISMA requirements included the *Contractor Systems* and *Incident Response and Reporting* metric categories. Specifically, the *ODNI Incident Management and Response Standard Operating Procedure* created by MSD provides the steps to address adverse incidents to include malicious code attacks, unauthorized access to ODNI systems, and unauthorized utilization of ODNI services, general misuse, and hoaxes. Additionally, the document provides links to the Intelligence Community Incident Response Center (IC-IRC) SharePoint site and includes email addresses and phone numbers needed for reporting and coordinating incidents with CIA Computer Incident Response Team, ISG, IC-IRC, and the Federal Bureau of Investigation (FBI) Enterprise Security Operations Center.⁴

~~(U//FOUO)~~ Furthermore, MSD officials are coordinating with a representative from Intelink to create an ODNI incident tracking database that will allow for: internal tracking for all ODNI incidents from start to finish, tracking numbers of incidents, the ability to see the history of incidents to identify repeat offenders, and an accurate account of tickets currently open or during a specified timeframe.⁵

~~(U//FOUO)~~ Also noted during this year's evaluation was the IC CIO's Authorization to Operate (ATO) the ODNI Information Assurance Management System, a workflow management tool for completing the risk management process. Although the workflow tool is still undergoing testing, once it is finalized, the tool should help ODNI with system authorization reciprocity, IC IT

⁴ ~~(U//FOUO)~~ The CIA Computer Incident Response Team and ISG are responsible for cleanup requests for incidents on the Agency Internet Network (AIN) and Common Workgroup Environment (CWE). The IC-IRC is responsible for the central management and coordination activity for IC incident handling and response. The FBI Enterprise Security Operations Center is the law enforcement entity for reporting incidents.

⁵ ~~(U//FOUO)~~ The Intelink Service Management Center, formerly known as Intelink Enterprise Collaboration Center or Intelligence Community Enterprise Solutions, is the organizational entity responsible for delivering the capability commonly known as Intelink. Intelink provides SharePoint hosting across the IC to enable sharing of ideas, information, and documents.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

registry reports, and standardization within the community for body of evidence documentation, risk management framework process development, and accreditation boundary information.

~~(U//FOUO)~~ The remainder of this report will discuss the FISMA metric areas in need of improvement. Annex B includes the matrix of the FY 2012 FISMA metrics for the ODNI and the IC IG conclusions for each.

1. (U) Continuous Monitoring Management

(U) The FY 2012 IG FISMA metrics require OIGs to evaluate the agency's continuous monitoring program. Continuous monitoring is the management and tracking of the security status of an organization's information systems. The objective of a continuous monitoring program is to determine the continued effectiveness for a complete set of deployed security controls within an information system. Continuous monitoring allows an organization to track the security state of an information system on an ongoing basis and is an established method for assessing the security impacts of changes, either planned or not, to the hardware, software, firmware, or environment of operation on information systems. The goal of continuous monitoring is to provide greater transparency on the health and status of information systems and operations with timely reporting of concerns. Understanding the security state of information systems is essential in dynamic environments of operation with changing threats, vulnerabilities, and technologies.

~~(U//FOUO)~~ In August 2008, the CIA and ODNI signed a memorandum of agreement (MOA) for the provision of mission support and infrastructure services by CIA to the ODNI. The MOA requires an annual fiscal year contract, Service Agreement (SA), between the CIA and ODNI to define the scope, frequency, and costs for the provided support. For the FY 2012 FISMA evaluation, we reviewed the SA for Information Technology Support provided by the CIA's Directorate of Support Office of Global Infrastructure.

~~(S//NF)~~ (b)(1) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] f

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1)



~~(U//FOUO)~~ **Impact of Not Having Continuous Monitoring Management.** As organizations become more dependent upon information technology for their mission critical functions, the confidentiality, integrity, and availability of information is critical. Without continuous monitoring, it is difficult to assess whether security controls within an information system continue to be effective over time, due to changes that occur in the normal course of business. Furthermore, the assessment of security impacts from planned and unplanned changes is also important, and without continuous monitoring, organizations will be unable to track the ongoing security state of an information system. Without employing a strategy for information security continuous monitoring, organizations may be unable to maintain an ongoing awareness of information security, vulnerabilities, and threats to support risk management decisions, which could be detrimental to operations.

Recommendation 1:

~~(U//FOUO)~~ Within 30 days of this report, the Director of the Mission Support Division should ensure that the FISMA continuous monitoring requirements are conveyed to the Infrastructure Services Group and that requirements are implemented.

~~(U//FOUO)~~ **Management Response.** MSD concurred with the recommendation. On 7 November 2012, MSD officials met with the ISG Chief to reemphasize ISG's role regarding continuous monitoring requirements and the necessary communication that must take place to implement such monitoring. MSD plans to document the meeting in an e-mail and provide a copy to the IC IG. See Appendix C for management comments in their entirety.

2. (U) Security Configuration Management

(U) Security Configuration Management is the process of overseeing hardware, software, firmware, and documentation changes in an effort to protect an information system from unacceptable modifications during the life of the system. FISMA requires each agency to establish a configuration management

⁶ ~~(U//FOUO)~~ Per an agreement between the CIA's Offices of Global Infrastructure and Global Communication Services and the ODNI, the FY 2011 SA terms and conditions are in effect until the FY 2012 SA is signed.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

program that is consistent with OMB policy, as well as applicable National Institute for Standards and Technology (NIST) guidelines. Specifically, the FY 2012 IG FISMA metrics require IGs to evaluate if the agency's configuration management program includes the following attributes:

- Documented policies and procedures.
- Defined standard baseline configuration.
- Assessment for compliance with baseline configuration.
- Timely remediation of scan result deviations.
- Implementation of secure configuration settings and documented deviations.
- Documented proposed and actual configuration changes.
- Implemented software assessment capability.
- Developed patch management process.

~~(U//FOUO)~~ The FY 2011 SA states that the ISG will develop and manage the configuration management program to include:

- Defining the standard baseline for all ODNI systems.
- Overseeing change and configuration control for ODNI systems.
- Preparing quarterly, as needed, presentations of system status and changes through MSD processes and boards.
- Maintaining overall configuration management documentation.
- Maintaining data center drawings.
- Performing scans of ODNI systems to ensure baseline compliance.

~~(U//FOUO)~~ ISG officials from the Operations and Maintenance Division were not aware of any baseline configuration scans that were performed to ensure baseline configuration compliance and stated that they had not seen the FY 2011 SA. In addition to meeting with ISG, we also met with MSD and IC CIO representatives about configuration management. Similar to the SA, MSD created a security configuration management guidelines document, dated 29 June 2012, that also lists the configuration management roles and responsibilities; however, those guidelines had not been communicated to the ODNI System Owners, MSD Information Technology, MSD Security, National Counterterrorism Center, National Counterintelligence Executive, or ISG staff performing configuration management duties.

~~(U//FOUO)~~ In addition to the lack of communicating the configuration management requirements, MSD and ISG did not have a timely process to approve the yearly service agreement to meet the criteria set forth by the mission support and infrastructure services MOA. The FY 2011 SA was signed

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

in November 2011, which is the second month of FY 2012 and the FY 2012 SA was still not signed as of July 2012. The MOA states that the ODNI shall provide its requirements for CIA goods and services to the CIA mission support service providers by 1 June every year. Any updates should be made between 1 June and 1 October so the CIA and ODNI can negotiate and execute the SA. Based on that criterion:

- The FY 2011 SA should have been signed by October 2010, but was not finalized until November 2011.
- The FY 2012 SA was required to be signed by October 2011; however, it had still not been signed by either the CIA or ODNI officials as of July 2012.

(U//~~FOUO~~) Importance of Having an Established Configuration

Management Program. According to NIST, because of frequent changes experienced by information system configurations, the controls in the configuration management family are considered a good example of volatile controls.⁷ A successful configuration management program can reduce the volatility by providing oversight and documentation of all modifications that occur for an information system in relation to hardware, software, and firmware. Although the FY 2011 SA remains effective until the FY 2012 SA is signed, the FY 2011 SA may not encompass changes to ODNI's support requirements for configuration management. Similarly, the lack of communication of the ODNI configuration management program leaves ODNI systems exposed to configuration-related vulnerabilities and could compromise the availability, integrity, and reliability of the systems.

Recommendation 2:

(U//~~FOUO~~) Within 30 days of this report, the Director of the Mission Support Division should disseminate and discuss the *Security Configuration Management Guidelines* to ISG officers responsible for its implementation.

(U//~~FOUO~~) Management Response. MSD concurred with the recommendation. On 7 November 2012, MSD officials met with the ISG Chief to reemphasize ISG's role regarding security configuration management requirements. MSD plans to document the meeting in an e-mail and provide a copy to OIG.

⁷ (U) NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation 3:

(U//~~FOUO~~) Within 180 days of this report, the Director of the Mission Support Division should develop a project timeline for defining and updating the requirements of the Service Agreement between MSD and ISG. This timeline should ensure the Service Agreement is signed and conveyed to the responsible offices by the start of the fiscal year for which it applies.

(b)(5) [Redacted]

3. (U) Risk Management

(U) The risk management process defined by the FY 2012 IG FISMA metrics requires an organization to conduct risk assessments, implement a strategy to mitigate risks, and utilize continuous monitoring techniques and procedures to evaluate the security of its information systems. Specifically, the metrics outline the following attributes for a risk management program:

- Documented and centrally located policies and procedures for risk management.
- Addresses risk from an organization perspective.
- Addresses risk from a mission and business process perspective.
- Addresses risk from an information system.
- Categorizes information systems in accordance with government policies.
- Selects an appropriately tailored set of baseline security controls.
- Implements the tailored set of baseline security controls.
- Assesses the security controls using appropriate assessment procedures.
- Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation.
- Ensures information security controls are monitored on an ongoing basis.
- Ensures information system specific risks (tactical), mission/business specific risks (operational), and organizational level risks (strategic) are communicated to appropriate levels of the organization.
- Ensures Senior Officials are briefed on threat activity on a regular basis by appropriate personnel.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- Prescribes the active involvement of stakeholders in the ongoing management of information system-related security risks.
- Ensures security authorization packages contain system security plan, security assessment report, and POA&M.
- Ensures security authorization packages contain accreditation boundaries for organization information systems.

(U//~~FOUO~~) This year, in order to gain a better understanding of the risk management process, we selected 4 different types of systems out of the 24 listed in the 18 June ODNI system inventory submission, to include a server, a network, an enclave, and an application. Those systems varied from a protection level (PL) 2 through a PL4 with confidentiality, integrity, and availability levels-of-concern (LOCs) ranging from high to low. Table 1 lists the four systems chosen for the FY 2012 evaluation.

(U) **Table 1: FY 2012 Systems Reviewed**

(b)(1)

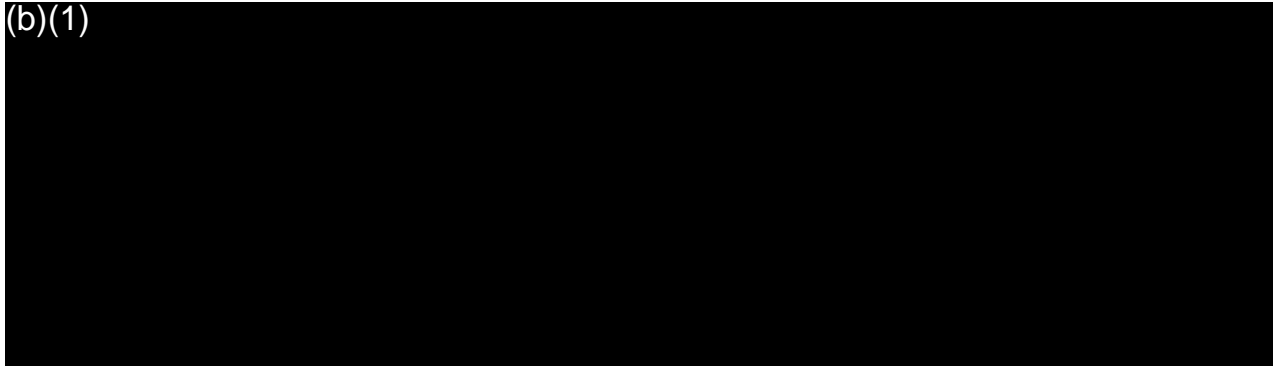


Table 1 is classified CONFIDENTIAL//NOFORN

(U) Source: MSD System Inventory Dated 30 June 2012

(b)(1)



⁸ (U) The risk management process was previously the certification and accreditation process.

⁹ (U) An SSP is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1)

~~(U//FOUO)~~ **Impact of Systems Operating Without Having an Approval to Operate.** Mission and business functions of organizations are dependent upon information technology and information systems. However; information systems are susceptible to internal and external threats, and Government information systems are not immune. Government information systems face serious threats that could adversely affect mission, Government operations, and the nation. Those threats could stem from environmental hazards, attacks, and human or machine errors that could result in serious damage to national and economic security.

~~(U//FOUO)~~ Without a systematic process to ensure that ODNI systems receive accreditations or reviews in a timely manner, shortfalls and vulnerabilities may not be identified and risks may not be properly assessed, which could result in exposure to intrusions and the potential loss of sensitive national security information.

Recommendation 4:

~~(U//FOUO)~~ Within 30 days of this report, the Intelligence Community Chief Information Officer, in coordination with the Director of the Mission Support Division should implement a process to communicate information systems risk to the appropriate level in the organization and document risk acceptance or include a schedule for re-authorization for systems that do not have authorization to operate.¹⁰

~~(U//FOUO)~~ **Management Response.** The IC CIO concurred with and provided a plan to address the recommendation. MSD concurred with the recommendation and will coordinate with the IC CIO to address ODNI specific-systems and develop a Standard Operating Procedure by 31 Jan 2013.

4. (U) Plan of Action and Milestones (POA&M)

(U) On 17 October 2001, OMB issued Memoranda 02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," which defined the purpose of a POA&M as a tool to assist agencies in identifying,

¹⁰ ~~(U//FOUO)~~ On 17 December 2008, the DNI delegated accreditation authority to the Associate Director of National Intelligence and Chief Information Officer (IC CIO) for all information systems under the authority of the DNI.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

assessing, prioritizing, and monitoring the progress of corrective actions for systems and program security weaknesses. The POA&M is one of the key documents in an information system's security authorization package and outlines the weaknesses identified, as well as the tasks that are planned to remediate the deficiencies noted during the security control assessment. For the FY 2012 IG FISMA metrics, IGs were asked to review the following attributes of a POA&M program:

- Ensures policies and procedures are documented for managing IT security weaknesses discovered during security control assessments and requiring remediation.
- Tracks, prioritizes, and remediates weaknesses.
- Ensures remediation plans are effective for correcting weaknesses.
- Establishes and adheres to milestone remediation dates.
- Ensures resources are provided for correcting weaknesses.
- Ensures POA&Ms include security weaknesses discovered during assessments of security controls that require remediation.
- Ensures costs associated with remediating weaknesses are identified.
- Ensures program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

~~(U//FOUO)~~ For our evaluation, we reviewed the POA&Ms for the four systems we selected for the Risk Management metric. In addition to the system level POA&Ms reviewed, MSD officials also provided a copy of the ODNI POA&M process document. This document provided the ODNI procedures for managing known IT security weaknesses, to include the requirement of the Information System Security Manager (ISSM) to track, prioritize, and remediate those weaknesses. Additionally, the process document states that ODNI ISSM should:

- Establish and adhere to reasonable remediation dates.
- Ensure that remediation plans are effective for correcting weaknesses.
- Ensure that adequate resources are provided for correcting weaknesses.
- Report on a regular basis, at least quarterly to the CIO.

~~(U//FOUO)~~ The POA&Ms we reviewed were not completed in accordance with the OMB or the MSD POA&M process. For example, the Office of Legislative Affairs Congressional Action Tracking System (OLA CATS) POA&M did not list the points of contact or resources required for the identified weaknesses; the ODNI Chief Human Capital Officer IC Capabilities Catalog (IC3) POA&M did not

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

have any data in the Milestones (required actions) column; and although the IC CIO reviewed and documented progress of remediation activity through the Security Assessment Report, neither MSD nor the IC CIO provided documentation to support regular, consistent communication or central tracking of POA&M activities.

(U) Impact of Incomplete POA&Ms. If a POA&M is incomplete and/or is not centrally managed, agencies may not be able to identify, assess, prioritize, or monitor the progress of corrective efforts, which could leave the agency programs or systems vulnerable to information security weaknesses.

Recommendation 5:

~~(U//FOUO)~~ Within 60 days of this report, the Director of the Mission Support Division should provide documentation to support that approved policies and procedures for managing IT security weaknesses that require remediation are being communicated. That documentation should outline how the staff is being educated on: completing the POA&M template, defining milestones dates, and identifying resources needed to accomplish the remediation plan within the milestone dates.

(U) Management Response. MSD concurred with the recommendation and stated it conducted information sessions with the Information System Security Officers on POA&M requirements and proper completion.

Recommendation 6:

~~(U//FOUO)~~ Within 90 days of this report, the Intelligence Community Chief Information Officer should develop a POA&M review process and document the status of remediation activities. That process should be performed by the IC CIO at least quarterly to provide the CIO the ability to centrally track and validate the progress of POA&M activities.

~~(U//FOUO)~~ **Management Response:** The IC CIO concurred with the recommendation. The Chief, Risk Management and Information Security Branch, will develop a POA&M review process to oversee the remediation of findings associated with ODNI-owned and managed information systems.

5. (U) Contingency Planning

~~(U//FOUO)~~ FISMA requires agencies to have contingency plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. A contingency/disaster recovery plan is a

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

strategy or organized course of action that is taken if things do not go as planned or if there is a loss of use of business systems due to a disaster. Contingency plans are developed to facilitate responses to anything that may have an impact on normal operations.

(U) For FY 2012, the IG FISMA metrics require that OIGs evaluate the agency's contingency planning program, which includes the following attributes:

- A documented business continuity and disaster recovery policy that provides the authority and guidance necessary to reduce the impact of a disruptive event or disaster.
- Ensures the organization has performed an overall Business Impact Analysis.
- Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures.
- Testing of system-specific contingency plans.
- Ensures documented business continuity and disaster recovery plans are in place and can be implemented when necessary.
- A developed and fully implementable testing, training, and exercise programs.
- Performance of regular ongoing testing or exercises of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.
- After-action reports that address issues identified during contingency/disaster recovery exercises.
- Systems that have alternate processing sites.
- Alternate processing sites that are subject to the same risks as primary sites.
- Backups of information that are performed in a timely manner.
- Contingency planning that considers supply chain threats.

~~(S//NF)~~ (b)(1) [Redacted text block]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1)



(C//NF) (b)(1)



(U) Table 2: Summary of System Contingency Plans

(b)(1)

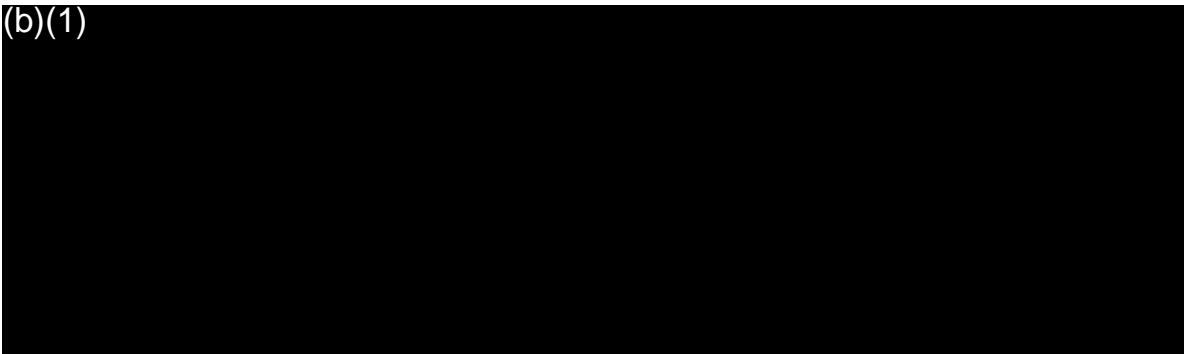


Table 2 is classified SECRET//NOFORN

(U) Source: MSD System Inventory Dated 30 June 2012

~~(S//NF)~~ (b)(1)



~~(U//FOUO)~~ Overall, the documentation provided did not indicate that ODNI had an adequate contingency plan program for its information systems. Based on our meetings with the ISG Operations and Maintenance Division officers and

¹¹ ~~(U//FOUO)~~ Director of Central Intelligence Directive 6/3, section 6.B.2.b and 6.B.3.b states that assurance shall be provided for systems operating at a medium or high Level-of-Concern for availability to include a contingency/disaster recovery plan.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

ODNI ISSM staff, there was a lack of awareness of roles and responsibilities for communication and implementation of contingency planning program requirements and oversight.

~~(U//FOUO)~~ Impact of Not Having Contingency Planning in Place.

Information systems are vulnerable to a variety of disruptions such as short-term power outage, disk drive failure, equipment destruction, or fire; therefore, an organization must have the ability to withstand disruptions and sustain its mission. Contingency plans are designed to guide personnel in the restoration of normal operations and describe strategies for ensuring the recovery of operations in accordance with defined objectives and timeframes. If a disaster strikes the workplace and a contingency plan is not in place, it is highly unlikely that normal business processes could easily and quickly be restored.

Recommendation 7:

~~(U//FOUO)~~ Within 180 days of this report, the Director of the Mission Support Division should create and disseminate the ODNI business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster to the ODNI systems.

~~(U//FOUO)~~ Management Response. MSD concurred with the recommendation. MSD is coordinating with the ODNI Mission Assurance Office to review a plan to mitigate the impact of a disruptive event or disaster to ODNI systems. MSD will provide a draft of the plan by 28 Feb 2013.

Recommendation 8:

~~(U//FOUO)~~ Within 180 days of this report, the Director of the Mission Support Division should establish a contingency plan program including, at a minimum, the areas outlined in the FY 2012 IG FISMA metrics and applicable system authorization policy.

~~(U//FOUO)~~ Management Response. MSD concurred with the recommendation and stated that it will coordinate with the Mission Assurance Officer and ISG to develop a contingency plan for ODNI critical systems. MSD will provide a draft contingency plan by 28 Feb 2013.

6. (U) Security Capital Planning

(U) According to NIST, IT security and capital planning and investment control processes have historically been completed by security and capital planning specialists; however, FISMA requires agencies to combine IT security into the

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

capital planning process.¹² This integration enables agencies to document resources and funding for IT security and risk management. Security Capital Planning is a new metric for the FY 2012 IG FISMA metrics. For this metric category, IGs were asked to evaluate the Security Capital Planning Program based on the following attributes:

- Documented policies and procedures exist to address information security in the capital planning and investment control process.
- Information security requirements are included as part of the capital planning and investment process.
- A discrete line item for information security is established in organizational programming and documentation.
- A business case/Exhibit 300¹³/Exhibit 53¹⁴ is employed to record the required information security resources.
- Information security resources are available for expenditure as planned.

(U//~~FOUO~~) The ODNI did not have an IT security capital planning and investment program for information security. MSD and IC CIO officials were not aware of a budget or any money being allocated for future information security; therefore, they were unable to provide the documentation to support a Security Capital Planning Program.

(U) Impact of Not Having a Security Capital Planning Program. According to NIST, without a strong and consistently applied capital planning process, project managers are more likely to:

- Assign inadequate resources to mitigate or resolve major risks.
- Make key decisions without adequate information.
- Have little insight into potential problems.
- Repeat mistakes that plagued earlier projects.
- Devote resources to addressing problems rather than avoiding them in the first place.
- Fail to deliver a compliant product or service on time and within budget.

¹² (U) NIST SP 800-65, "Integrating IT Security into the Capital Planning and Investment Control Process", January 2005.

¹³ (U) Exhibit 300 is the document OMB uses to assess and make funding decisions on IT investments.

¹⁴ (U) Exhibit 53 provides an overview of an agency's IT portfolio.

~~SECRET//NOFORN~~

Recommendation 9:

(U//~~FOUO~~) Within 240 days of this report, the Director of the Mission Support Division should establish a security capital planning and investment program for information security including, at a minimum, the areas outlined in the FY 2012 IG FISMA metrics.

(U//~~FOUO~~) Management Response. MSD concurred with the recommendation and stated that a security capital planning and investment program for information security will be in the FY 2014 Congressional Budget Justification Book and will provide a copy by 31 December 2012.

7. (U) Systems Inventory

(U) FISMA provides a framework to ensure that agencies and departments implement effective measures to secure Federal Government information and information systems. A complete and accurate inventory of systems is imperative to properly manage information systems.

(U) For FY 2012 FISMA reporting purposes, IGs were asked to review the organization’s systems inventory to include the documentation of agency and contractor systems, systems ATOs, security controls test dates, and systems contingency plan testing.

(U//~~FOUO~~) During our review of the ODNI systems inventory, MSD provided five different inventories with varying degrees of consistency or completeness. A summary of the numbers of systems in the inventories provided is in Table 3.

(U) Table 3: Systems Inventory Submission Summary

Date of Inventory	Date Provided	Number of Systems
30 April 2012	31 May 2012	42
30 May 2012	31 May 2012	25
6 June 2012	6 June 2012	76
18 June 2012	18 June 2012	24
30 June 2012	2 July 2012	24
Table 3 is UNCLASSIFIED//FOR OFFICIAL USE ONLY		

(U) Source: MSD FISMA SharePoint Site

~~(S//NF)~~ (b)(1) [Redacted]

[Redacted]

[Redacted]

~~SECRET//NOFORN~~

(b)(1)



~~(U//FOUO)~~ In addition to a review of the current system inventory, we also reviewed the ODNI's inventory located in the Intelligence Community Information Technology (IC/IT) Registry. The IC/IT Registry is a central repository where the inventories of the entire IC are consolidated. The IC CIO is responsible for maintaining the IC/IT Registry and for compiling FISMA information from members of the IC into a comprehensive annual report to OMB and Congress. MSD officials are responsible for uploading the ODNI system inventory information into the IC/IT Registry on at least a quarterly basis for FISMA reporting purposes. However, the ODNI internal system inventory has not aligned to the inventory in the IC/IT Registry dating back to the FY 2009 FISMA review. During our evaluation this year, the ODNI inventory in the IC/IT Registry still did not reflect the internal system inventory provided by MSD officials. An IC CIO representative stated that the IC/IT Registry had an issue with the uploading capability and was coordinating with the MSD ISSM to remediate the issue.

(U) Impact of System Inventory Inaccuracies. An inaccurate system inventory hinders the ODNI's ability to ensure that system security measures are addressed or that critical systems are accounted for and secure.

Recommendation 10:

~~(U//FOUO)~~ Within 90 days of this report, the Director of the Mission Support Division should create and disseminate a repeatable system inventory tracking process with procedures for tracking all systems that require an ATO.

~~(U//FOUO)~~ **Management Response.** MSD concurred with the recommendation and plans to establish, provide, and distribute via the Security Management Oversight Board and the Cyber Security Program board, a repeatable system inventory tracking process for all systems requiring an ATO by 31 January 2013, with a copy to the OIG for review.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation 11:

~~(U//FOUO)~~ Within 180 days of this report, the Intelligence Community Chief Information Officer should execute an agreement with the CIA CIO for reporting and monitoring ODNI-owned systems that are accredited through the CIA accreditation processes.

(U) Management Response: The IC CIO concurred with the recommendation and stated they will work with MSD and the CIA to address this recommendation.

Recommendation 12:

~~(U//FOUO)~~ Within 180 days of this report, the Director of MSD should ensure that internal MSD inventories are consistent with the IC/IT Registry to include system additions, deletions, or adjustments on at least a quarterly basis.

(U//~~FOUO~~) Management Response. MSD concurred with the recommendation and by 1 December 2012, MSD, in coordination with IC CIO, will validate and post on the FISMA SharePoint site the current quarterly submission to verify that the ODNI systems inventory is up to date and reflects accurately the current ODNI systems inventory.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

V. (U) Follow-Up on Open Recommendations

(U//~~FOUO~~) In June 2011, Intelink transitioned to NSA through an MOU between the ODNI and NSA, and 32 open recommendations were provided to the NSA OIG for consideration. In October 2012, the NSA OIG initiated an audit to determine if the deficiencies identified in the FY 2011 FISMA report were still present. Following our discussion with the NSA OIG, the 32 open recommendations for Intelink were administratively closed for ODNI.

(U) Since July 2011, ODNI has closed 17 recommendations from the FY 2009, FY 2010, and FY 2011 FISMA reports. MSD provided documentation to close 12 of the 17 recommendations: 2 were from the FY 2009 report, 5 from the FY 2010 report, and 5 from the FY 2011 report. The IC CIO closed the remaining five recommendations: one from FY 2009 and four from FY 2010. By closing those recommendations, the ODNI has improved the security controls testing process, accreditation policy and procedure documentation, security configuration management oversight, and the incident response and reporting program.

(U//~~FOUO~~) Two recommendations remain open from the FY 2011 FISMA report and address the need to have an accurate systems inventory and policies and procedures for a continuous monitoring program. FISMA reporting serves as a foundation for ensuring that agencies monitor and provide strong oversight of their systems' security and the data that resides on those systems. This is particularly important for IC agencies given their respective missions. Without adequately addressing security concerns, ODNI systems could be vulnerable to attacks.

(U) The summary of open and recently closed recommendations for FY 2009 is shown in Table 4.

(U) Table 4: FY 2009 FISMA Recommendations

Table 4 is UNCLASSIFIED// FOR OFFICIAL USE ONLY	
Recommendation	Status
1.2. (U// FOUO) Reconcile the systems' inventories with the IC IT Registry, at a minimum, on a quarterly basis	MSD CLOSED
5.0.a. (U// FOUO) Develop a uniform written plan of action and milestone process for the ODNI.	CIO CLOSED
6.2.a. (U// FOUO) The Mission Support Center (MSC) and IECC should adopt and implement Federal Desktop Core Configuration	MSD CLOSED

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table 4 is UNCLASSIFIED// FOR OFFICIAL USE ONLY	
Recommendation	Status
(FDCC) standard configurations and document deviations and security control deficiencies on desktops directly controlled by ODNI. ¹⁵	
6.2.b. (U// FOUO) Implement FDCC security settings into all Windows XP™ and Vista™ desktops directly controlled by the ODNI.	MSD CLOSED

(U) Source: IC IG

(U) The summary of open and recently closed recommendations for FY 2010 is shown in Table 5.

(U) Table 5: FY 2010 FISMA Recommendations

Table 5 is UNCLASSIFIED// FOR OFFICIAL USE ONLY	
Recommendation	STATUS
1.1.b. (U// FOUO) Reconcile MSC internal inventories with the IC IT Registry and make system additions, deletions, or adjustments to the IC IT Registry at a minimum on a quarterly basis.	MSD CLOSED
2.3. (U// FOUO) Formalize and document the process as well as perform security tests on the systems that currently have security tests that are greater than 1-year old.	MSD CLOSED
4.1.a. (U// FOUO) Revise the security configuration management oversight program for its systems that includes OMB's FY 2010 FISMA requirements.	MSD CLOSED
4.1.c. (U// FOUO) Establish responsibility for those CM functions that MSC will not include in the Service Agreement with ISG.	MSD CLOSED
4.1.d. (U// FOUO) Ensure the proper implementation of FDCC standards according to the milestones established for intelligence agencies and document deviations from those standards when appropriate.	MSD CLOSED
4.2.a. (U// FOUO) Establish a security configuration management program for its systems that meets OMB's FY 2010 FISMA requirements.	CIO CLOSED
5.2.a. (U// FOUO) Finalize its draft Intelink Incident Response Plan	CIO CLOSED

¹⁵ (U) MSC transitioned to the Mission Support Division (MSD) in November 2010.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table 5 is UNCLASSIFIED// FOR OFFICIAL USE ONLY	
Recommendation	STATUS
and ensure that it meets or exceeds all requirements established by OMB and FISMA.	
5.2.b. (U// FOUO) Establish an incident response and reporting program that meets OMB's expectations for comprehensive analysis, validation, documentation, and resolution of incidents in a timely manner timely reporting of incident data to appropriate authorities.	CIO CLOSED
6.2. (U// FOUO) Develop a written POA&M program for the IECC. Repeats 2009 Recommendation 5 a, b, c, due to be completed in November 2009.	CIO CLOSED
7.1. (U// FOUO) Establish and document a continuous monitoring program incorporating all of OMB's requirements.	MSD CLOSED

(U) Source: IC IG

(U) The summary of open and recently closed recommendations for FY 2011 is shown in Table 6.

(U) Table 6: FY 2011 FISMA Recommendations

Table 6 is UNCLASSIFIED// FOR OFFICIAL USE ONLY	
Recommendation	Status
1.1. (U// FOUO) Perform an assessment of the network scans provided by ISG at least annually to validate MSD systems inventory.	MSD OPEN
2.1. (U// FOUO) Formalize and document the process as well as perform security tests on the systems that currently have security tests that are greater than 1-year old.	MSD CLOSED
3.1. (U// FOUO) Refine and develop MSD's certification and accreditation policies and procedures documentation to ensure that they describe all roles and responsibilities in the certification and accreditation process.	MSD CLOSED
4.1.a. (U// FOUO) Revise the security configuration management oversight program for its systems that includes FY 2011 OIG FISMA metric requirements.	MSD CLOSED
4.1.b. (U// FOUO) Establish responsibility for those CM functions that MSD will not include in the Service Agreement with ISG.	MSD CLOSED

~~SECRET//NOFORN~~

Table 6 is UNCLASSIFIED// FOR OFFICIAL USE ONLY	
Recommendation	Status
4.1.c. (U// FOUO) Ensure the proper implementation of FDCC standards according to the milestones established for intelligence agencies and document deviations from those standards.	MSD CLOSED
6.1. (U// FOUO) Update the continuous monitoring policy and procedure documentation to ensure that it addresses the FY 2011 FISMA metric criteria. Finalize all documentation and indicate approval with a signature and date.	MSD OPEN

(U) Source: IC IG

~~SECRET//NOFORN~~

(U) Appendix A: Acronyms

ATO	Authorization to Operate
CIA	Central Intelligence Agency
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DNI	Director of National Intelligence
FBI	Federal Bureau of Investigation
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC IG	Office of the Inspector General of the Intelligence Community
IC IRC	Intelligence Community Incident Response Center
IC/IT Registry	Intelligence Community /Information Technology Registry
ICCS	Intelligence Community Cyberscope
ICD	Intelligence Community Directive
IECC	Intelink Enterprise Collaboration Center (Intelink)
ISG	Infrastructure Services Group
ISSM	Information System Security Manager
IT	Information Technology
LOC	Level of Concern
MOA	Memorandum of Agreement
MSD	Mission Support Division
NIST	National Institute for Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PL	Protection Level
POA&M	Plan of Action and Milestones
SA	Service Agreement
SP	Special Publication
SSP	System Security Plan

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~**(U) Appendix B: FY 2012 IG FISMA Metrics Results**Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

1. Continuous Monitoring		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation." If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
1.1. Has the Organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		No
1.1.1.	Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). (AP)	Yes
1.1.2.	Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G). (AP)	No
1.1.3.	Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST SP 800-53A). (AP)	No
1.1.4.	Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as Plan of Action and Milestone (POA&M) additions and updates with the frequency defined in the strategy and/or plans (NIST SP 800-53, NIST SP 800-53A). (AP)	No
Explanation:		
1.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was <u>not noted</u> in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

2. Security Configuration Management		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation." If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
2.1. Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		No
2.1.1.	Documented policies and procedures for configuration management. (Base)	Yes
2.1.2.	Standard baseline configurations defined. (Base)	Yes
2.1.3.	Assessing for compliance with baseline configurations. (Base)	No
2.1.4.	Process for timely, as specified in Organization policy or standards, remediation of scan result deviations. (Base)	No

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

2. Security Configuration Management		
2.1.5.	For Windows-based components, Federal Desktop Core Configuration (FDCC)/ United States Government Configuration Baseline (USGCB) secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented. (Base)	N/A (explain)
2.1.6.	Documented proposed or actual changes to hardware and software configurations. (Base)	Yes
2.1.7.	Process for timely and secure installation of software patches. (Base)	Yes
2.1.8.	Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). (Base)	No
2.1.9.	Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2). (Base)	No
2.1.10.	Patch management process is fully developed, as specified in Organization policy or standards. (NIST SP 800-53: CM-3, SI-2). (Base)	Yes
(U// FOUO) Explanation: 2.1.5 - During the FY 2011 FISMA evaluation, the ISG representative provided documentation to support that the baseline FDCC baseline settings were implemented. This year we did not test to ensure that the FDCC had been fully implemented, so we are marking this N/A.		
2.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED)

3. Identity and Access Management		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
3.1. Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:		N/A (explain)
3.1.1.	Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). (Base)	N/A (explain)
3.1.2.	Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST SP 800-53, AC-2). (Base)	N/A (explain)
3.1.3.	Identifies when special access requirements (e.g., multi-factor authentication) are necessary. (Base)	N/A (explain)
3.1.4.	If multi-factor authentication is in use, it is linked to the Organization's Personal Identity Verification (PIV) program where appropriate (NIST SP 800-53, IA-2).(KFM)	N/A (explain)
3.1.5.	Organization has adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). (AP)	N/A (explain)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table is classified: (UNCLASSIFIED)

3. Identity and Access Management		
3.1.6.	Ensures that the users are granted access based on needs and separation of duties principles. (Base)	N/A (explain)
3.1.7.	Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts) (Base)	N/A (explain)
3.1.8.	Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users) (Base)	N/A (explain)
3.1.9.	Ensures that accounts are terminated or deactivated once access is no longer required. (Base)	N/A (explain)
3.1.10.	Identifies and controls use of shared accounts. (Base)	N/A (explain)
(U) Explanation: Overall, the ODNI follows the CIA's policies and procedures for account and identity management and CIA's Infrastructure Services Group manages the oversight of these policies for ODNI owned systems. This metric category will be reviewed by the CIA IG as a part of their FISMA evaluation.		
3.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

4. Incident Response and Reporting		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
4.1. Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		Yes
4.1.1.	Documented policies and procedures for detecting, responding to and reporting incidents (NIST SP 800-53: IR-1). (Base)	Yes
4.1.2.	Comprehensive analysis, validation and documentation of incidents. (KFM)	Yes
4.1.3.	When applicable, reports to US Computer Emergency Readiness Team (US-CERT) within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). (KFM)	Yes
4.1.4.	When applicable, reports to law enforcement within established timeframes (NIST SP 800-86). (KFM)	Yes

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

4. Incident Response and Reporting		
4.1.5.	Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST SP 800-53, NIST SP 800-61, and OMB M-07-16, M-06-19). (KFM)	N/A (explain)
4.1.6.	Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. (Base)	N/A (explain)
4.1.7.	Is capable of correlating incidents. (Base)	N/A (explain)
4.1.8.	There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, NIST SP 800-61, and OMB M-07-16, M-06-19). (Base)	Yes
(U// FOUO) Explanation: 4.1.5. - The example provided did not have a time frame associated, therefore we could not ascertain if it met criteria. 4.1.6 - The ODNI does not have a cloud environment. 4.1.7 - We did see the ODNI correlation of incidents, but the IC IRC posts information about all incidents occurring in the IC for all IC members to review.		
4.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

5. Risk Management		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
5.1. Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		Yes
5.1.1.	Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. (Base)	Yes
5.1.2.	Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev.1 (Base)	N/A (explain)
5.1.3.	Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST SP 800-37, Rev.1. (Base)	N/A (explain)
5.1.4.	Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1. (Base)	N/A (explain)
5.1.5.	Categorizes information systems in accordance with government policies. (Base)	Yes
5.1.6.	Selects an appropriately tailored set of baseline security controls. (Base)	Yes
5.1.7.	Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. (Base)	N/A (explain)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

5. Risk Management		
5.1.8.	Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)	Yes
5.1.9.	Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. (Base)	N/A (explain)
5.1.10.	Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. (Base)	Yes
5.1.11.	Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization. (Base)	No
5.1.12.	Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., Chief Information Security Officer (CISO)). (Base)	Yes
5.1.13.	Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks. (Base)	Yes
5.1.14.	Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, NIST SP 800-37) (Base)	Yes
5.1.15.	Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies. (Base)	Yes
(U// FOUO) Explanation: 5.1.2., 5.1.3., 5.1.4., 5.1.7., and 5.1.9. are all part of the ICD 503 risk management framework that has not been implemented by the IC CIO.		
5.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED)

6. Security Training	
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.	Answer
6.1. Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:	N/A (explain)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table is classified: (UNCLASSIFIED)

6. Security Training		
6.1.1.	Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1). (Base)	N/A (explain)
6.1.2.	Documented policies and procedures for specialized training for users with significant information security responsibilities. (Base)	N/A (explain)
6.1.3.	Security training content based on the organization and roles, as specified in Organization policy or standards. (Base)	N/A (explain)
6.1.4.	Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Organization users) with access privileges that require security awareness training. (KFM)	N/A (explain)
6.1.5.	Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training. (KFM)	N/A (explain)
6.1.6.	Training material for security awareness training contains appropriate content for the Organization (NIST SP 800-50, NIST SP 800-53). (Base)	N/A (explain)
Explanation: (U) Explanation: This metric is N/A for the ODNI since they follow CIA policies and procedures for Security Training and this metric will be reviewed as part of the CIA IG's FISMA evaluation.		
6.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

7. Plan of Action & Milestones (POA&M)		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
7.1. Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		No
7.1.1.	Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation. (Base)	Yes
7.1.2.	Tracks, prioritizes and remediates weaknesses. (Base)	Yes
7.1.3.	Ensures remediation plans are effective for correcting weaknesses. (Base)	No
7.1.4.	Establishes and adheres to milestone remediation dates. (Base)	No
7.1.5.	Ensures resources are provided for correcting weaknesses. (Base)	No

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

7. Plan of Action & Milestones (POA&M)		
7.1.6.	POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25). (Base)	No
7.1.7.	Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25). (Base)	No
7.1.8.	Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25). (Base)	No
Explanation:		
7.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED)

8. Remote Access Management		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
8.1. Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		N/A (explain)
8.1.1.	Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17). (Base)	N/A (explain)
8.1.2.	Protects against unauthorized connections or subversion of authorized connections. (Base)	N/A (explain)
8.1.3.	Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1). (Base)	N/A (explain)
8.1.4.	Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). (Base)	N/A (explain)
8.1.5.	If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3). (KFM)	N/A (explain)
8.1.6.	Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)	N/A (explain)
8.1.7.	Defines and implements encryption requirements for information transmitted across public networks. (KFM)	N/A (explain)
8.1.8.	Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required. (Base)	N/A (explain)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table is classified: (UNCLASSIFIED)

8. Remote Access Management		
8.1.9.	Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3, US-CERT Incident Reporting Guidelines). (Base)	N/A (explain)
8.1.10.	Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). (Base)	N/A (explain)
8.1.11.	Remote access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6). (Base)	N/A (explain)
(U) Explanation: The Remote Access Program metric category is not applicable to the ODNI since the ODNI does not use remote access.		
8.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

9. Contingency Planning		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
9.1. Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		No
9.1.1.	Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1). (Base)	Yes
9.1.2.	The Organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34). (Base)	No
9.1.3.	Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34). (Base)	No
9.1.4.	Testing of system specific contingency plans. (Base)	No
9.1.5.	The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (Federal Continuity Directive 1 (FCD1), NIST SP 800-34). (Base)	N/A (explain)
9.1.6.	Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	Yes
9.1.7.	Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans. (Base)	No
9.1.8.	After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)	N/A (explain)
9.1.9.	Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	No

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

9. Contingency Planning		
9.1.10.	Alternate processing sites are subject to the same risks as primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53)	No
9.1.11.	Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	Yes
9.1.12.	Contingency planning that consider supply chain threats. (Base)	N/A (explain)
(U// FOUO) Explanation: 9.1.5 - Backup and Recovery SOP and the example provided did not provide enough information to determine if the plan can be implemented when necessary. 9.1.8. - the latest exercise was too new for an after action report to have been completed, however, during the FY 2011 FISMA evaluation ISG personnel provided a lessons learned document. 9.1.12 - Supply Chain threats are new and the criteria was not finalized in time for agency implementation and IG evaluation.		
9.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Contingency Planning Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

10. Contractor Systems		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
10.1.	Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:	Yes
10.1.1.	Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud. (Base)	N/A (explain)
10.1.2.	The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines. (Base)	Yes
10.1.3.	A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud. (Base)	Yes
10.1.4.	The inventory identifies interfaces between these systems and Organization-operated systems (NIST SP 800-53: PM-5). (Base)	Yes
10.1.5.	The Organization requires appropriate agreements (e.g., Memorandums of Understanding (MOUs), Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. (Base)	N/A (explain)
10.1.6.	The inventory of contractor systems is updated at least annually. (Base)	Yes

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

10. Contractor Systems		
10.1.7.	Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. (Base)	Yes
(U// FOUO) Explanation: 10.1.1. - ODNI follows CIA procedures. 10.1.5. - No agreements are required for the IDEAS system.		
10.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

11. Security Capital Planning		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
11.1. Has the Organization established a security capital planning and investment program for information security? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:		No
11.1.1.	Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.(Base)	No
11.1.2.	Includes information security requirements as part of the capital planning and investment process. (Base)	No
11.1.3.	Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). (Base)	No
11.1.4.	Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). (Base)	No
11.1.5.	Ensures that information security resources are available for expenditure as planned. (Base)	No
Explanation:		
11.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.		
Explanation:		

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

12. System Inventory		
Please select Yes, No, or Not Applicable (N/A) from the pull down menu. If N/A is selected, please provide a brief explanation in the space labeled "Explanation". If more than one attribute is N/A, please label each explanation with the corresponding attribute number.		Answer
12.1. Has the Organization established a systems inventory for information security? If yes, besides the improvement opportunities that may have been identified by the OIG, does the inventory include the following attributes:		No

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Table is classified: (UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

12. System Inventory		
12.1.1.	Documented number of agency and contractor systems	No
12.1.2.	Documented number of systems with a security Authorization to Operate (ATO)	Yes
12.1.3.	Documented security controls test date	Yes
12.1.4.	Documented number of systems with a tested contingency plan	No
Explanation:		
12.2. (OPTIONAL) Please provide any additional information on the effectiveness of the Organization's System Inventory that was not noted in the questions above.		
Explanation:		

~~SECRET//NOFORN~~

(U) Appendix C: Management Comments

(U) Mission Support Division and the IC CIO provided the following comments to the proposed recommendations:

Recommendation 1:

~~(U//FOUO)~~ Within 30 days of this report, the Director of the Mission Support Division should ensure that the FISMA continuous monitoring requirements are conveyed to the Infrastructure Services Group and that requirements are implemented.

_____ XX _____ **Concur** _____ **Non-concur**

(U//~~FOUO~~) Comments: To address this recommendation, MSD met with C/ISG on 7 November 2012 to reemphasize ISG’s role regarding security configuration management and continuous monitoring requirements and the necessary communication that must take place to implement such monitoring. MSD will document this meeting in an e-mail and provide a copy to OIG, particularly focusing on how monitoring will be implemented through the Security Configuration and Management Guide, which contains continuous monitoring requirements.

(U) MSD provided OIG hard copies of the security configuration management and Continuous Monitoring Guidelines to OIG representatives on 8 November 2012. Both documents are posted in the FISMA SharePoint site.

Recommendation 2:

~~(U//FOUO)~~ Within 30 days of this report, the Director of the Mission Support Division should disseminate and discuss the Security Configuration Management Guidelines to ISG officers responsible for its implementation.

_____ XX _____ **Concur** _____ **Non-concur**

(U) Comments: See comments in response to Recommendation #1 to address this recommendation.

Recommendation 3:

~~(U//FOUO)~~ Within 180 days of this report, the Director of the Mission Support Division should develop a project timeline for defining and updating the requirements of the Service Agreement between MSD and ISG. This timeline should ensure the Service Agreement is signed and conveyed to the responsible offices by the start of the fiscal year for which it applies.

XX **Concur** Non-concur

~~(U//FOUO)~~ **Comments:** MSD is currently coordinating the FY 13 SAs with GCS and ISG. Plan is to

- Input the draft SA into the SA SharePoint site by 20 Nov.
- Complete CIA and ODNI reviews by 15 Dec.
- CIA and ODNI signatures by 31 Dec.

~~(U//FOUO)~~ The MSD plan for the FY 14 SAs:

- Begin FY 14 negotiations in June 2013.
- Input the draft SA into the SA SharePoint site by 31 July.
- Complete CIA and ODNI reviews by 15 Sep.
- CIA and ODNI signatures by 30 Sep.

Recommendation 4:

~~(U//FOUO)~~ Within 90 days of this report, the Intelligence Community Chief Information Officer, in coordination with the Director of the Mission Support Division should implement a process to communicate information systems risk to the appropriate level in the organization and document risk acceptance or include a schedule for re-authorization for systems that do not have authorization to operate.

XX **Concur** Non-concur

~~(S//NF)~~ **Comments:** (b)(1) [Redacted]

(b)(1)

(U) MSD will coordinate with IC CIO to address ODNI specific systems and develop a Standard Operating Procedure by 31 Jan.

Recommendation 5:

~~(U//FOUO)~~ Within 60 days of this report, the Director of the Mission Support Division should provide documentation to support that approved policies and procedures for managing IT security weaknesses that require remediation are being communicated. That documentation should outline how the staff is being educated on: completing the POA&M template, defining milestones dates, and identifying resources needed to accomplish the remediation plan within the milestone dates.

XX **Concur** **Non-concur**

(U) Comments: MSD conducted information sessions with the ISSOs on POA&M requirements and proper completion in July 2012. Minutes from this meeting were provided to all ISSOs by e-mail in early August. The POA&M is posted on the FISMA SharePoint site for review.

Recommendation 6:

~~(U//FOUO)~~ Within 90 days of this report, the Intelligence Community Chief Information Officer should develop a POA&M review process and document the status of remediation activities. That process should be performed by the IC CIO at least quarterly to provide the CIO the ability to centrally track and validate the progress of POA&M activities.

XX **Concur** **Non-concur**

~~(U//FOUO)~~ **Comments:** The Chief, Risk Management and Information Security Branch, under the DNI Chief Information Security Officer, will develop a POA&M review process to oversee the remediation of findings associated with ODNI owned and managed information systems (DNI Systems). The process will use the DNI Assessment and Risk Management Application (DARMA) that will track the security authorizations, to include POA&Ms for all DNI systems and will include a tickler system to help reinforce periodic reviews of remediation activities. The CISO will schedule quarterly reviews with the MSD ISSM to review progress on open POA&M's.

Recommendation 7:

(U//~~FOUO~~) Within 180 days of this report, the Director of the Mission Support Division should create and disseminate the ODNI business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster to the ODNI systems.

_____ XX _____ **Concur** _____ **Non-concur**

(U//~~FOUO~~) Comments: MSD Security and IT are coordinating with the ODNI Mission Assurance Office to review a plan to mitigate the impact of a disruptive event or disaster to ODNI systems. MSD will provide a draft of the plan by 28 Feb 2013.

Recommendation 8:

(U//~~FOUO~~) Within 180 days of this report, the Director of the Mission Support Division should establish a contingency plan program including, at a minimum, the areas outlined in the FY 2012 IG FISMA metrics and applicable system authorization policy.

_____ XX _____ **Concur** _____ **Non-concur**

(U) Comments: MSD/IT will coordinate with the Mission Assurance Officer and GCS/ISG to develop a contingency plan for ODNI critical systems. MSD will provide a draft contingency plan by 28 Feb 2013.

Recommendation 9:

(U//~~FOUO~~) Within 240 days of this report, the Director of the Mission Support Division should establish a security capital planning and investment program for information security including, at a minimum, the areas outlined in the FY 2012 IG FISMA metrics.

_____ XX _____ **Concur** _____ **Non-concur**

(U//~~FOUO~~) Comments: MSD will include a security capital planning and investment program for information security in the FY 14 CBJB and provide a copy by 31 Dec 2012.

~~SECRET//NOFORN~~

Recommendation 10:

~~(U//FOUO)~~ Within 90 days of this report, the Director of the Mission Support Division should create and disseminate a repeatable system inventory tracking process with procedures for tracking all systems that require an ATO.

XX **Concur** Non-concur

~~(U//FOUO)~~ **Comments:** MSD will establish, provide, and distribute via the Security Management Oversight Board and the Cyber Security Program board, a repeatable system inventory tracking process for all systems requiring an ATO by 31 Jan 2013, with a copy to the OIG for review.

Recommendation 11:

~~(U//FOUO)~~ Within 180 days of this report, the Intelligence Community Chief Information Officer should execute an agreement with the CIA CIO for reporting and monitoring ODNI-owned systems that are accredited through the CIA accreditation processes.

XX **Concur** Non-concur

~~(S//NF)~~ (b)(1) [Redacted]

~~(S//NF)~~ (b)(1) [Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation 12:

~~(U//FOUO)~~ Within 180 days of this report, the Director of MSD should ensure that internal MSD inventories are consistent with the IC/IT Registry to include system additions, deletions, or adjustments on at least a quarterly basis.

XX _____ **Concur** _____ **Non-concur**

~~(U//FOUO)~~ **Comments:** In response to this recommendation and to ensure the accuracy of future quarterly validations, by 1 Dec 2012, MSD in coordination with IC CIO, will validate and post on the FISMA SharePoint site the current quarterly submission to verify that the ODNI systems inventory is up to date and reflects accurately the current ODNI systems inventory. MSD will verify systems inventories with the IC/IT Registry quarterly and post the IC IT registry snapshots of ODNI's system inventory on the FISMA SharePoint site for OIG review.

~~SECRET//NOFORN~~