



Evaluation Report
OFFICE OF THE INSPECTOR GENERAL OF THE
INTELLIGENCE COMMUNITY

**(U) Fiscal Year 2011 Independent Evaluation of ODNI Compliance with the
Federal Information Security Management Act of 2002**

AUD-2012-003

28 December 2011

(U//~~FOUO~~) Table of Contents

- (U) Executive Summary 3
- (U) Objective 5
- (U//~~FOUO~~) Scope and Methodology..... 5
- (U) Background 5
- (U) FISMA Reporting Changes 7
- (U//~~FOUO~~) Evaluation Results..... 9
 - (U) Systems Inventory 10
 - (U//~~FOUO~~) Finding 1: MSD and Intelink Have Not Validated Their Systems Inventory, and Intelink is Not Maintaining an Accurate Inventory. 10
 - (U//~~FOUO~~) Finding 2: MSD and Intelink Have Not Conducted Required Annual Security Controls Testing..... 13
 - (U) Certification and Accreditation..... 18
 - (U//~~FOUO~~) Finding 3: MSD and Intelink Have Established Certification and Accreditation (C&A) Programs But Still Need to Make Improvements Based on C&A Metric Criteria. . 18
 - (U) Security Configuration Management..... 23
 - (U) Finding 4: MSD and Intelink are Performing Some Security Configuration Management (CM) Functions, But a Required Configuration Management Program is Not Yet in Place. 23
 - (U) Remote Access..... 26
 - (U) Finding 5: Intelink Does Not Currently Have a Sufficient Remote Access Program.. 26
 - (U) Continuous Monitoring..... 27
 - (U//~~FOUO~~) Finding 6: MSD Needs to Make Improvements to Their Continuous Monitoring Program and Intelink Does Not Have an Adequate Continuous Monitoring Program..... 27
 - (U) Contingency Planning..... 29
 - (U//~~FOUO~~) Finding 7: Intelink Does Not Have Required Contingency Planning Programs or Contingency Plans 29
- (U) Follow-Up on FY 2008 FISMA Recommendations 32
- (U) Follow-Up on FY 2009 FISMA Recommendations 33
- (U) Follow-Up on FY 2010 FISMA Recommendations 36
- (U) Annex A: List of Acronyms 40

~~SECRET//NOFORN~~

(U) Annex B: Matrix of ODNI OIG FY 2011 FISMA Recommendations 42

~~(S//NF)~~ Annex C: FY 2011 OIG FISMA Metrics for MSD..... 44

~~(S//NF)~~ Annex D: FY 2011 OIG FISMA Metrics for Intelink..... 56

(U//~~FOUO~~) Table of Figures

Table 1: ~~(S//NF)~~ Security Testing Status of MSD FISMA Reportable Information Systems..... 14

Table 2: ~~(S//NF)~~ Security Testing Status of Intelink FISMA Reportable Information Systems.. 15

Table 3: ~~(S//NF)~~ C&A Status of MSD Information Systems Reported for FISMA Purposes 20

Table 4: ~~(S//NF)~~ C&A Status of Intelink Information Systems Reported for FISMA Purposes . 20

Table 5: ~~(S//NF)~~ Contingency Plan and Contingency Plan Test Status of Intelink Information Systems Reported for FISMA Purposes 30

Table 6: (U//~~FOUO~~) Status of FY 2008 FISMA Recommendations 32

Table 7: (U//~~FOUO~~) Status of FY 2009 FISMA Recommendations 34

Table 8: (U//~~FOUO~~) Status of FY 2010 FISMA Recommendations 36

Table 9: (U//~~FOUO~~) Status of FY 2011 FISMA Recommendations 42

~~SECRET//NOFORN~~

(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. 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. Within the ODNI, two groups are responsible for information systems: the Mission Support Division (MSD), which is responsible for internal ODNI systems, and the Intelink Enterprise Collaboration Center (Intelink), which is responsible for Intelligence Community (IC) systems. The senior officials for these organizations are the Director, Mission Support Division (D/MSD) and the Intelligence Community Chief Information Officer (IC CIO), respectively. The specific purpose of this evaluation was to determine the adequacy of the information security programs for MSD and Intelink. To perform the evaluation, we applied the Office of Management and Budget's (OMB) Fiscal Year (FY) 2010 FISMA metrics for 11 categories of information security, titled as the FY 2011 IG FISMA metrics and followed up on progress made by MSD and Intelink to address recommendations made in the OIG's FY 2008, FY 2009, and FY 2010 FISMA reports.¹

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



(U//~~FOUO~~) Since issuing the FY 2010 FISMA report, the ODNI has closed a total of 40 recommendations from our FY 2008, FY 2009, and FY 2010 FISMA reports. These recommendations were designed to reduce the vulnerability of ODNI systems to attack and compromise of critical information. Implementation of these recommendations has improved the accuracy of the ODNI's system inventories, clarified responsibilities for IT security, strengthened

¹ (U) As of 8 November 2011, the Intelligence Community Inspector General (ICIG) was sworn in replacing what was formerly the ODNI OIG.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

the ODNI's incident response and reporting program, and facilitated the planning and performance of contingency plan tests on IT systems. The ODNI, in particular MSD, has continued to make progress toward ensuring that it has an effective information security program.

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

[Redacted]

(U//) (b)(5)

[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Objective

(U//~~FOUO~~) The objective of this review was to provide an independent evaluation of the ODNI information security program and practices as required by FISMA of 2002. 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 recommendations made in the OIG's FY 2008, FY 2009, and FY 2010 FISMA reports.

(U//~~FOUO~~) Scope and Methodology

(U) We performed this review from March 2011 through July 2011, 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 our evaluation objectives. In order to satisfy OMB reporting requirements and milestones, we could not wait until the FY 2011 FISMA metrics were finalized. As a result, we evaluated the adequacy and effectiveness of the ODNI's information security programs in accordance with OMB's FY 2010 FISMA metrics as identified by the CIGIE Federal Audit Executive Council (FAEC). In addition, we reviewed steps taken to implement the recommendations in the OIG's previous FY 2008, FY 2009, and FY 2010 FISMA reports.

(U//~~FOUO~~) (b)(3)



(U//~~FOUO~~) To achieve the evaluation objective, we reviewed information and documentation provided to us by MSD, Intelink, and ICIA officials. Information included internal policies and procedures; ODNI's internal systems inventories from MSD and Intelink; certification and accreditation (C&A) data for selected systems; system security test information; systems' contingency plans and contingency plan testing procedures; plans of action and milestones (POA&M) for systems; and security configuration management (CM), incident reporting, and security awareness training procedures.

(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

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

operations and assets.² FISMA compliance is a matter of national security and therefore 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 Chief Information Officer (CIO) and calls for agency CIOs to implement FISMA provisions through agency information security officers. As the head of the IC, the Director of National Intelligence (DNI) has delegated this authority to the IC CIO to ensure compliance with this legislation for the IC. The IC CIO is the senior official who heads the Office of the IC CIO.

(U) Based on the ODNI ownership interests in the information systems, MSD and Intelink are the two groups that maintain internal inventories for their respective organizations.³ The two organizations are responsible for uploading their system inventory information into the Intelligence Community/Information Technology (IC/IT) Registry on at least a quarterly basis for FISMA reporting purposes. The IC/IT Registry is a central repository where the inventories of the entire IC are consolidated. The IC CIO office is responsible for maintaining the IC/IT Registry and for compiling FISMA information from members of the IC into a comprehensive annual report that is sent to OMB and Congress.

(U) At the end of FY 2010, the former IC IT Registry was decommissioned as it was no longer supported by the vendor and was no longer capable of capturing the required data elements. A new IC IT Registry was procured, deployed, and ultimately received Authorization to Operate (ATO) on 13 June 2011. Following this authorization, the Intelligence Community Information Assurance (ICIA) division issued a data call to all of the IC members requesting that they submit their systems inventory data by 17 June 2011 to establish a new Registry baseline.

(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.⁴ For an agency with an Office of the Inspector General (OIG) appointed under the Inspector General Act of 1978, that independent evaluation is performed annually by the OIG or by an

² (U) Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et. seq

³ (U) 44 U.S.C. § 3545

⁴ (U//~~FOUO~~) Intelink is a group within the IC CIO office that maintains one of the two internal inventories of ODNI-owned systems. For the remainder of the report we will refer to the IC CIO and Intelink Enterprise Collaboration Center collectively as the Intelink.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

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 would include the ODNI, only an entity designated by the agency head may perform the independent evaluation. In ODNI Instruction 2005-10, *Inspector General of the Office of the Director of National Intelligence*, 7 September 2005, the DNI authorized the ODNI OIG to perform the independent evaluations.⁵

(U//~~FOUO~~) In prior years, the IC CIO instructed the OIGs, or independent evaluators within the IC, to forward their completed evaluations to the IC CIO. However, as of 15 September 2010, the IC OIGs forwarded their completed reports to the ODNI OIG.⁶ The reports address the progress made toward remedying security weaknesses and the overall effectiveness of the information technology security program based on metrics received from OMB.⁷

(U//~~FOUO~~) During our review this year, Intelink officials reported that ODNI and National Security Agency (NSA) management developed a Memorandum of Understanding (MOU) to transfer services, resources, and personnel supporting Intelink from ODNI to the NSA. However, since an agreement had not been signed at the start of review, we continued to evaluate Intelink as a part of the ODNI independent evaluation.

(U) FISMA Reporting Changes

(U) OMB Annual FISMA Instructions through FY 2008. Since the passage of FISMA in 2002 and through FY 2008, OMB has published on its website detailed annual FISMA reporting instructions for Federal agencies. Each year, OMB has issued instructions that included templates (Excel spreadsheets) for agency CIOs, OIGs, and Senior Agency Officials for Privacy (SAOP). The templates consisted of questions and responses to be used in completing the CIO, OIG, and SAOP assessments. Upon completion of the templates, Federal agencies forwarded to OMB the templates along with any written reports on issues identified during their reviews. OMB then compiled all the information into a consolidated report submitted to Congress the following March. The agencies’ FISMA reports were due to OMB generally by

⁵ (U) As of 8 November 2011, the Intelligence Community Inspector General (ICIG) was sworn in replacing what was formerly the ODNI OIG.

⁶ (U//~~FOUO~~) Prior to FY 2010, the IC CIO received the IC CIO, OIG, and the Senior Agency Official for Privacy (SAOP) reports and consolidated the reports into an annual IC FISMA report. Beginning with FY 2010, the ODNI OIG consolidated the IC OIG reports and submitted them separately to Congressional oversight committees and OMB.

⁷ (U//~~FOUO~~) Since the implementation of OMB’s electronic database in FY 2009, OMB no longer issues the FISMA instructions to agencies in memorandum form. The metrics are now included in OMB’s CyberScope database. OMB made its draft FY 2010 FISMA metrics available to the IC OIGs in April 2010. Due to time constraints and lack of new guidance, ODNI OIG circulated the FY 2010 FISMA metrics in April 2011 to the IC OIGs with guidance to use them in conducting their FY 11 evaluations under the title FY 2011 IG FISMA Metrics.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1 October. Within the IC, the IC agencies forwarded their FISMA reports to the IC CIO. All the IC agencies' CIO, OIG, and SAOPs' reports were then consolidated into an annual IC report by the IC CIO and submitted to OMB and Congress.

(U) Changes to FISMA Requirements for FY 2009, FY 2010, and FY 2011. Since FY 2008, OMB has 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 (referred to as CyberScope), which is an unclassified automated reporting tool.⁸ For FY 2009, OMB required federal agencies, including the CIOs, OIGs, and SAOPs, to obtain OMB's annual instructions and metrics from CyberScope. Agencies were instructed to enter the results of their annual FISMA reviews online to enable OMB to directly upload the data. However, the IC was, and continues to be, unable to use the database due to the classified nature of its FISMA information. Therefore, for FY 2009 and FY 2010, the IC OIGs provided their reports to OMB via classified channels. FY 2011 reports will be processed in the same manner. IC CIO officials anticipate having a classified system with the CyberScope capabilities in place for FY 2012 FISMA reporting.

(U) OMB modified the metrics used by agencies for FY 2010 to perform their FISMA evaluations. Specifically, the new metrics used by OIGs now focus on an evaluation of the agency's security programs and their implementation. The focus in the past centered on multiple choice responses which were designed to broadly evaluate an agency's security. OMB's goal was to determine if processes were working effectively to safeguard information and information systems. These revisions were designed to shift the focus of OIGs' FISMA evaluations away from being largely a culture of "paperwork" reports and toward implementing solutions that actually improve security.

(U) On 21 April 2010, OMB issued Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, to agency CIOs, OIGs, and SAOPs. This memorandum consisted of four pages of FISMA requirements for FY 2010 and a series of "frequently asked questions" relating to the new OMB CyberScope database. The OMB metrics for CIOs, OIGs, and SAOPs were also included in the CyberScope database.

(U) As of 7 April 2011, representatives from the Department of Homeland Security (DHS) and the CIGIE had not finalized the FISMA OIG metrics to be used for FY 2011. As a result, on 7 April 2011, in order to meet reporting deadlines, the ODNI OIG issued the

⁸ (U) The OMB database was originally known as the CyberSecurity Automated Repository and Management Application. The name of the database was changed to CyberScope, which is how the system is referred to in this report.

~~SECRET//NOFORN~~

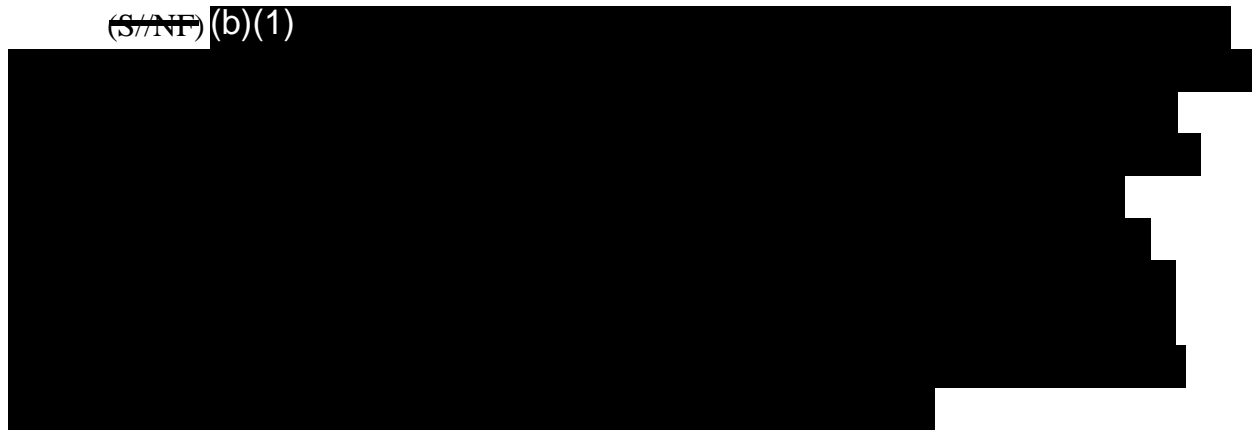
~~SECRET//NOFORN~~

memorandum for FY 2011 Federal Information Security Management Act Guidance for Offices of the Inspector General in the Intelligence Community which identified the OMB FY 2010 FISMA metrics as the FY 2011 OIG FISMA metrics. These metrics require that OIGs report on their agencies' performances in 11 program areas, which include the following:

1. System Inventory⁹
2. Certification and Accreditation (C&A)
3. Security Configuration Management (CM)
4. Incident Response and Reporting
5. Security Training
6. Plans of Action and Milestones (POA&M)
7. Remote Access
8. Account and Identity Management
9. Continuous Monitoring
10. Contingency Planning
11. System Contractor Oversight

~~(U//FOUO)~~ Evaluation Results

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



~~(U//FOUO)~~ (b)(3)



⁹ (U) Information should include the following for the information systems inventory: Impact Level/Level of Concern, number of agency systems, number of contractor systems, systems certified and accredited, number of systems that have had annual testing, and testing of contingency plans.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(3)

(U//~~FOUO~~) Annexes C and D include matrices of the FY 2011 FISMA metrics for MSD and Intelink and the OIG conclusions for each.

(U) Systems Inventory

(U//~~FOUO~~) Finding 1: MSD and Intelink Have Not Validated Their Systems Inventory, and Intelink is Not Maintaining an Accurate Inventory.

(U//~~FOUO~~) 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. The OIG's FY 2008, 2009, and 2010 FISMA reports made recommendations to MSD and Intelink for improving their inventories. MSD and Intelink took steps during and after our FY 2010 FISMA evaluation to reconcile and improve the accuracy of their inventories as discrepancies were identified and recommendations issued.

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

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

¹⁰ ~~(S//NF)~~ (b)(1)

~~SECRET//NOFORN~~

(b)(1)



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



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



~~(U//FOUO)~~ **IC/IT Registry.** At the end of FY 2010 the old IC IT Registry was decommissioned as it was no longer supported by the vendor and was no longer capable of

¹¹ (U) A computer system parent-child relationship is determined by the connectivity, interoperability, and the definition of boundaries of the systems. The parent-child relationship is interconnected and supports a common mission or function. Child systems are within the same boundaries and are considered part of the parent system. For example, a child system may contain databases from which the parent is able to make queries.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

capturing the required data elements. A new IC IT Registry was procured, deployed, and received Authorization to Operate (ATO) on 13 June 2011. Following this authorization, the Intelligence Community Information Assurance (ICIA) division issued a data call to all of the IC members requesting they submit their systems inventory data by 17 June 2011 to establish a new Registry baseline.

(U//~~FOUO~~) The OIG's FY 2009 and 2010 FISMA reviews revealed that MSD and Intelink maintained inaccurate system inventories within the IC/IT registry. Since the new IC IT registry did not receive an ATO until June 2011, we were not able to reconcile the provided internal inventory against the IC/IT registry for the FY 2011 FISMA evaluation.

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



(U//~~FOUO~~) **Impact of Not Monitoring Systems Connected to the Network.** The National Institute of Standards and Technology (NIST) Special Publication (SP) on Information Security Continuous Monitoring for Federal Information Systems and Organizations states “Information security is a dynamic process that must be effectively managed to respond to new vulnerabilities, evolving threats, and an organization’s constantly changing enterprise architecture and operational environment.”¹² Furthermore the publication defines information security continuous monitoring and indicates that this necessitates maintaining situational awareness of all systems and system configurations across the organization, maintaining an understanding of threats and threat activities, evaluating the security impact of actual and proposed changes, assessing all security controls, collecting, correlating and analyzing security-related information, providing actionable communication of security status across all levels of the organization, and active management of risk by organizational officials. In order for MSD and Intelink to improve their risk management program, they should validate that their system inventory is accurate and that no uncertified and unaccredited systems have been connected. Without this validation, the agency could be subjected to information security related risks due to the loss of confidentiality, integrity, or availability of information or information systems.

¹² (U) See the National Institute of Standards and Technology, NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U//~~FOUO~~) (b)(5)

[Redacted]

(U//~~FOUO~~) (b)(5)

[Redacted]

(U//~~FOUO~~) Recommendation 1.1

**Within 180 days of this report, the D/MSD should:
Perform an assessment of the network scans provided by the ISG at least annually to validate the MSD systems inventory.**

(U//~~FOUO~~) Recommendation 1.2

- Within 180 days of this report, the IC CIO should:**
- a. Assess systems inventory data by performing network scans at least annually to validate the Intelink systems inventory.**
 - b. Develop and maintain an accurate inventory of systems.**

(U//~~FOUO~~) Finding 2: MSD and Intelink Have Not Conducted Required Annual Security Controls Testing.¹³

(U//~~FOUO~~) According to the FY 2011 OIG FISMA metrics, OIGs are to report, for the systems identified in an agency's inventory, the number of systems for which security controls have been tested and reviewed. Security tests provide an analysis of the safeguards protecting an information system in a given operational environment for the purpose of determining the security posture of that system.

(U//~~FOUO~~) Intelligence Community Directive 503 and Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information with Information*

¹³ (U//~~FOUO~~) The D/MSD submitted documentation on 9 November 2011 as evidence of the security controls testing for all three FISMA reportable systems and the corresponding recommendation has been closed.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Systems, 5 June 1999, establish security policies and procedures for storing, processing, and communicating classified intelligence information in information systems.¹⁴ Therefore, they provide information concerning the testing of information systems to ensure that data are secure. In accordance with the DCID 6/3, all systems with a Protection Level (PL) greater than 1 should receive annual security testing. In addition, both MSD and Intelink issued information system security policies which state that systems shall be reviewed annually or whenever security-relevant changes occur, which is consistent with the requirements of DCID 6/3.

(U//~~FOUO~~) The rating levels are based on the required clearances, formal access approval, and a need-to-know basis of all direct and indirect users who receive information from the system without manual intervention and reliable human review. A system operates at PL 1 when all users have all the required approvals for access to all of the information in the system. A system operates at a PL 5 when at least one user lacks any clearance for access to some of the information on the system.

(U//~~FOUO~~) Based on documentation submitted by MSD and Intelink Information Systems Security Manager (ISSM) staff, we reviewed internal inventories to identify those systems that required security testing and to determine whether annual security tests were performed in accordance with DCID 6/3 and internal policies.

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

Table 1: (S//NF) (b)(1)

[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]

¹⁴ (U//~~FOUO~~) The IC CIO requires compliance with DCID 6/3 in addition to Intelligence Community Directive 503, which will not be fully phased in until FY 2014.

¹⁵ (S//NF) Neither MSD nor Intelink has any systems with PL ratings of either 1 or 5.

¹⁶ (U//~~FOUO~~) The D/MSD submitted documentation on 9 November 2011 as evidence of the security controls testing for all three FISMA reportable systems. The updated dates are 29 July 2011 and 26 Nov 2010 for the PL 3 systems. The PL 4 system also has an updated security controls test date of 15 July 2011.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

tests greater than one year old or no security testing at all. Without annual security tests, vulnerabilities may exist that could expose MSD and Intelink information systems to outside threats such as intrusions, attacks, or viruses. Therefore, it is imperative that the regular annual security testing processes be implemented.

(U//~~FOUO~~) (b)(5)

[Redacted]

(U//~~FOUO~~) (b)(5)

[Redacted]

(U//~~FOUO~~) Recommendation 2.1¹⁷

**Within 180 days of this report, the D/MSD should:
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.**

(U//~~FOUO~~) Recommendation 2.2

**Within 180 days of this report, the IC CIO should:
Perform security tests on the systems that currently have security tests that are greater than 1-year old.**

¹⁷ (U//~~FOUO~~) At the time the audit was completed, this recommendation was valid based on documentation provided to the OIG; however, on 9 November 2011 D/MSD provided additional documentation to support that all 3 FISMA reportable systems have had security controls testing within the last year. This recommendation has been closed.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~**(U) Certification and Accreditation****(U//~~FOUO~~) Finding 3: MSD and Intelink Have Established Certification and Accreditation (C&A) Programs But Still Need to Make Improvements Based on C&A Metric Criteria.**

(U//~~FOUO~~) Requirements for a C&A Program. According to the FY 2011 FISMA metrics, the OIG is to report on the status of the agency's C&A program which should include the following criteria:

1. Documented policies and procedures describing the roles and responsibilities of participants in the C&A process.
2. Established accreditation boundaries for agency information systems.
3. Categorization of information systems.
4. Application of applicable minimum baseline security controls.
5. Assessment of risks and tailored security control baseline for each system.
6. Assessment of the management, operational, and technical security controls in the information system.
7. Documentation in the system security plan, risk assessment, or equivalent document of the analyzed risks to agency operations, assets, or individuals.
8. Documentation that the accreditation official is provided with the following:
 - (i) security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective action;
 - (ii) plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and
 - (iii) updated system security plan with the latest copy of the risk assessment.

(U) The C&A process, from initial C&A to the withdrawal of accreditation, covers the entire life cycle of an information system. A C&A is a comprehensive process to ensure implementation of security measures that effectively counter relevant threats and vulnerabilities. The C&A process consists of several iterative, independent phases and steps whose scope and specific activities vary for the system that is being certified and accredited.

(U//~~FOUO~~) (b)5

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(5)



(U//~~FOUO~~) (b)(5)



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



¹⁸ (U) Documents required for C&A packages typically consist of system categorization statement, system description with system boundaries noted, network diagram and data flows, software and hardware inventory, business assessment risk, system risk assessment, contingency plan, self-assessment, and a system security plan.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- (b)(1) [Redacted]

[Redacted]

(U) Tables 3 and 4 provide details concerning the status of MSD's and Intelink's systems' accreditations

Table 3: ~~(S//NF)~~ C&A Status of MSD Information Systems Reported for FISMA Purposes

C&A Authorization Type	C&A Expiration Date	Total
ATO	4/26/2011	1
	5/30/2011	1
	7/24/2011	1
ATO Total		3
Grand Total		3

Source: ODNI OIG analysis of data from MSD

Table 4: ~~(S//NF)~~ C&A Status of Intelink Information Systems Reported for FISMA Purposes

C&A Authorization Type	C&A Expiration Date	Total
ATO	3/18/2007	1
	5/3/2007	1
	10/21/2007	1
	11/1/2007	1
	11/12/2007	1
	2/17/2008	2
	4/11/2008	1
	6/22/2008	3
	9/7/2008	1
	1/19/2009	1
	9/30/2009	1
	10/19/2009	1
	2/16/2010	1
	7/19/2010	1
	9/1/2010	1
	1/3/2011	1
	3/20/2011	1
	3/26/2011	2
	4/27/2011	1
	9/30/2011	1

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

C&A Authorization Type	C&A Expiration Date	Total
	10/29/2011	1
	12/23/2011	1
	3/4/2012	1
	5/4/2012	1
	6/8/2012	2
	7/21/2012	5
	7/23/2012	3
	8/5/2012	1
	8/27/2012	4
	10/14/2012	3
	11/2/2012	1
	11/3/2012	1
	3/1/2013	3
	4/22/2013	2
	5/11/2013	3
	6/11/2013	1
	6/29/2013	1
	6/30/2013	1
	9/1/2013	1
	10/20/2013	3
	4/1/2014	1
ATO Total		64
IATO	12/3/2004	3
	12/19/2007	1
IATO Total		4
IATT	5/11/2011	1
	6/21/2011	1
	8/11/2011	1
	10/7/2011	1
	11/3/2011	1
	12/1/2011	3
IATT Total		8
(blank)	(blank)	55
(blank) Total		55
Grand Total		131

Source: ODNI OIG analysis of data from Intelink

(U//~~FOUO~~) Impact of Systems Operating Without Current Accreditations. Intelink currently has 64 systems that are listed as having an ATO, further analysis of the inventory found that at least 6 of these systems had an expired ATO and the documentation provided did not list the system review date to substantiate that the ATO was still valid. Furthermore, 55 systems did

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

not have any information listed regarding accreditation status. Without a systematic process in place to ensure that the Intelink systems receive accreditations or reviews in a timely manner, shortfalls and vulnerabilities may not be identified and risks may not be properly assessed. This could result in exposure to intrusions and the potential loss of sensitive national security information.

(U//~~FOUO~~) Management Response. The D/MSD concurred with this recommendation. As of September 2011, MSD officials stated that they have updated and signed the C&A procedure which included specific roles and responsibilities as recommended by the OIG. The new procedure is posted on MSD's FISMA SharePoint site. The IC CIO concurs with recommendation 3.2 but indicated that 60 days would not allow for the required coordination and suggested changing the recommendation wording to "within 90 days of this report, the IC CIO should: Update the ODNI certification and accreditation process and procedure documentation to ensure that it addresses the metrics criteria, finalize all documentation, and indicate approval with a signature and date of the ATO of the ODNI Information Assurance Management System (OIAMS)." The IC CIO did not concur with recommendation 3.3 because the services, resources, and personnel supporting Intelink were transferred from ODNI to NSA on 1 Oct 2011; and they no longer have direct control over Intelink.

(U//~~FOUO~~) Audit Response. We will monitor MSD's progress to address this recommendation. The IC CIO concurred with recommendation 3.2. Even though the responsibility of Intelink was transferred to the NSA, the weaknesses revealed by our review and the corresponding recommendations may still be valid. We will meet with the NSA's IG office to discuss our review of Intelink and allow them to determine if these recommendations are still applicable.

(U//~~FOUO~~) Recommendation 3.1

Within 90 days of this report, the D/MSD should:

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.

(U//~~FOUO~~) Recommendation 3.2

Within 90 days of this report, the IC CIO should:

Update the certification and accreditation process and procedure documentation to ensure that it addresses the metric criteria, finalize all documentation, and indicate approval with a signature and date.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~**(U//~~FOUO~~) Recommendation 3.3**

**Within 60 days of this report, the IC CIO should:
Develop a C&A strategy, including a schedule for reaccrediting its systems.**

(U) Security Configuration Management**(U) Finding 4: MSD and Intelink are Performing Some Security Configuration Management (CM) Functions, But a Required Configuration Management Program is Not Yet in Place.¹⁹**

(U) FISMA requires each agency to develop minimally acceptable CM programs and ensure compliance with those programs.²⁰ The FY 2011 FISMA reporting metrics require OIGs to report on the extent to which agencies' security CM programs include the following:

- Documented policies and procedures.
- Establishment of, and compliance with, standard baseline configurations.
- Scans for compliance with baseline configurations.
- Implementation of Federal Desktop Core Configuration (FDCC) baseline settings and/or full documentation for any deviations from FDCC baseline settings.²¹
- Documented actual or proposed configuration changes.
- Established processes for the timely and secure installation of software patches.

(U//~~FOUO~~)(b)(3)

¹⁹ (U//~~FOUO~~) The D/MSD submitted documentation on 9 November 2011, thus the finding and related recommendations are no longer applicable for the FY 2011 review so the recommendation has been closed.

²⁰ (U) 44 U.S.C. § 3544(b)(2)(D)(iii)

²¹ (U) In August 2008, OMB issued OMB M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, directing the Federal government to adopt secure configurations of the FDCC. To address these requirements, ODNI Information Technology Governance Board initiated an Intelligence Community Tiger Team to measure and report compliance with FDCC. The Tiger Team developed a report that included revised milestones for intelligence agencies' implementation of the OMB requirements, stating that deployment should be completed by 30 June 2011; however, based on discussions with the IC CIO the deployment date has been modified to the end of September.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(3)



- | 
- | 
- | 

(U//~~FOUO~~) (b)(3)



(U) Intelink CM Program. Intelink has continued efforts to establish a security CM program; however, it is still developing the policies and procedures documents. Intelink provided the draft and signed Intelink *Configuration Management Plan* that includes establishing a configuration control board and developing a process for configuration monitoring and reporting. In addition to the configuration management plan, Intelink also has a configuration management policy and procedure directive that will establish the internal policy and procedures for managing Intelink information and technology configurations when it is signed and approved. The policy outlines the roles and responsibilities of the Intelink Configuration Control Board, Configuration Manager, Government division leads, and the technical writer.

(U//~~FOUO~~) Intelink FDCC Implementation. Intelink is working to ensure that its systems are compliant with OMB's FDCC implementation requirements for intelligence agencies. Intelink officials initially stated that they are working to implement Windows 7 by the end of July 2011; however, during our quarterly recommendation meeting in June 2011, Intelink officials modified the implementation date to the end of September.

(U//~~FOUO~~) Impact of the lack of a CM program. MSD and Intelink are taking actions to implement configuration management controls, including utilizing contractor support to perform CM functions and developing Configuration Management plans, policies, and procedures, however they need to finalize the aforementioned plans, policies, and procedures to

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

ensure that their security configuration management program that fully meets OMB and FISMA requirements. Until such programs are fully in place, ODNI is at increased risk that vulnerabilities that may be part of initial unidentified system baselines, those introduced during normal configuration changes, or those potentially introduced for malicious purposes could be exploited by threat-sources and compromise the availability, integrity, and reliability of IC-wide systems.

(U//~~FOUO~~) (b)(5)



(U//~~FOUO~~) (b)(5)



(U//~~FOUO~~) **Recommendation 4.1²²**

Within 120 days of this report, the D/MSD should:

- a. Revise the security configuration management oversight program for its systems that includes FY 2011 OIG FISMA metric requirements.**
- b. Establish responsibility for those CM functions that will not be covered by the Service Agreement with ISG.**
- c. Ensure the proper implementation of FDCC standards according to the milestones established for intelligence agencies and document any deviations from those standards.**

²² (U//~~FOUO~~) The D/MSD submitted documentation on 9 November 2011, thus the finding and related recommendations are no longer applicable for the FY 2011 review and have been closed.

~~SECRET//NOFORN~~

~~(U//FOUO)~~ Recommendation 4.2

Within 180 days of this report, the IC CIO should:

- a. Update the security configuration management policy and procedure documentation to ensure that it addresses the FY 11 FISMA metric criteria; finalize all documentation and indicate approval with a signature and date.
- b. Ensure the proper implementation of FDCC standards according to the milestones established for intelligence agencies and document any deviations from those standards when appropriate.

(U) Remote Access

(U) Finding 5: Intelink Does Not Currently Have a Sufficient Remote Access Program.

(U) **Intelink Remote Access Program.** The signed, April 2011 Intelink Access Policy does not sufficiently address the FY 2011 IG FISMA criteria for remote access programs. The policy states “Remote access to unclassified Intelink systems is available to eligible users on a case-by case basis based on operational need. Users requesting remote access are required to submit an application directly to Intelink.” However, to comply with the FY 2011 IG FISMA metric criteria for a remote access program, the policy must document the policies and procedures for authorizing, monitoring, and controlling all methods of remote access. Additionally, the remote access program should outline: how to protect against unauthorized connections, uniquely identify users, describe the authentication mechanisms, when users are required to encrypt transmitted files, and the maximum time of inactivity before re-authentication is required.

~~(U//FOUO)~~ **Impact of the lack of a Remote Access program.** An expanded access policy is needed to ensure that the remote access program meets OMB and FISMA requirements. Until such a program is fully in place, ODNI is at increased risk that facilities, networks, and devices may contain hostile threats that could expose DNI data and resources to unauthorized access.

~~(U//FOUO)~~ (b)(5)

[Redacted]

~~(U//FOUO)~~ (b)(5)

[Redacted]

~~SECRET//NOFORN~~

~~(U//FOUO)~~ Recommendation 5.1

**Within 120 days of this report, the IC CIO should:
Establish a remote access program including at a minimum, the areas outlined in
the FY 2011 OIG FISMA metrics.**

(U) Continuous Monitoring

**~~(U//FOUO)~~ Finding 6: MSD Needs to Make Improvements to Their Continuous
Monitoring Program and Intelink Does Not Have an Adequate Continuous Monitoring
Program.**

~~(U//FOUO)~~ The FY 2011 FISMA metrics require OIGs to evaluate the agency's continuous monitoring program. The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time due to changes that occur in the normal course of business. It is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation. Continuous monitoring allows an organization to track the security state of an information system on an ongoing basis. The goal of continuous monitoring is to provide greater transparency of the health and status of information systems and operations and timely reporting of concerns. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission.

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

[Redacted]

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

[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1)

(U//~~FOUO~~) **Impact of Not Having Continuous Monitoring in Place.** Continuous monitoring is the process and technology used to detect compliance and risk issues associated with an organization's operational environment. The operational environment consists of people, processes, and systems working together to support efficient and effective operations. Without a continuous monitoring program, it will be 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. The assessment of security impacts from planned and unplanned changes is important, and without continuous monitoring, organizations will be unable to track the security state of an information system on an ongoing basis.²³

(U//~~FOUO~~) (b)(5)

(U//~~FOUO~~) (b)(5)

²³ (U) Senator Joseph Lieberman and Representative Jane Harman introduced legislation, *Protecting Cyberspace as a National Asset Act of 2010*, in the United States Senate and House of Representatives, respectively. If passed, the legislation would update FISMA to require continuous monitoring. Specifically, the bills seek to increase the coordination of Federal agency activities and enhance situational awareness throughout the Federal government using more effective enterprise-wide automated monitoring, detection, and response capabilities. The Senate bill is S. 3480, and the House of Representatives bill is H.R. 5548.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(5)

(U//~~FOUO~~) Recommendation 6.1**Within 180 days of this report, the D/MSD should:****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.****(U//~~FOUO~~) Recommendation 6.2****Within 90 days of this report, the IC CIO should:****Establish and document a continuous monitoring program that incorporates all of the FY 11 FISMA metric requirements.****(U) Contingency Planning****(U//~~FOUO~~) Finding 7: Intelink Does Not Have Required Contingency Planning Programs or Contingency Plans**

(U) Contingency Planning Programs. FISMA requires agency contingency plan programs to have plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. The FY 2011 FISMA metrics require that OIGs evaluate the agency's contingency planning program which includes a plan and testing of that plan. The FY 2011 metrics criteria require attributes for a contingency planning program to include the following:

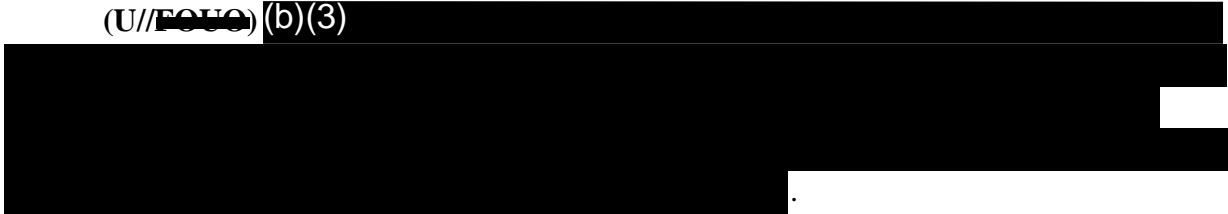
1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.
2. Performance of an overall Business Impact Assessment.
3. Development and documentation of division, component, and information technology infrastructure recovery strategies, plans, and procedures.
4. Testing of system specific contingency plans.
5. Documented business continuity and disaster recovery plans are ready for implementation.
6. Development of training, testing, and exercises approaches.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- 7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

(U//~~FOUO~~) (b)(3)



(U//~~FOUO~~) Contingency Plans. A contingency planning/disaster recovery plan is a 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. According to DCID 6/3 Section 6.B.2.b(1), contingency plans are required for all systems with availability Level-of-Concern ratings of medium or greater.²⁴ The Level-of-Concern is a rating assigned to each information system for confidentiality, integrity, and availability. The Level-of-Concern can be Basic, Medium, or High. The Level-of-Concern for availability is based on the needed availability of the information maintained, processed, or transmitted by the information system for mission accomplishment and how much tolerance is allowed for delay.

(U//~~FOUO~~) (b)(3)

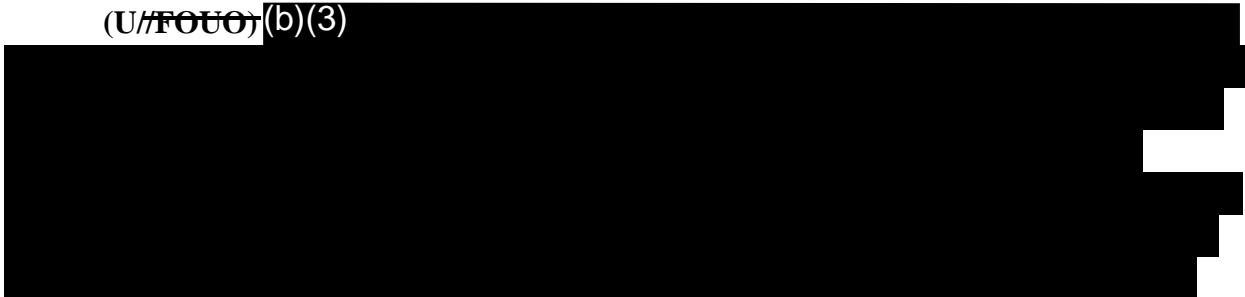


Table 5: (S//NF) (b)(1)

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

²⁴ (U//~~FOUO~~) Director of Central Intelligence Directive 6/3 Section 6.B.2.b(1), assurance shall be provided for systems operating at a medium Level-of-Concern for Availability; contingency planning that includes a contingency/disaster recovery plan.

~~SECRET//NOFORN~~**(U) Follow-Up on FY 2008 FISMA Recommendations**

(U//~~FOUO~~) Table 6 identifies recommendations made to MSD and Intelink in the ODNI OIG's FY 2008 annual FISMA report and the status of their implementation.

(U//~~FOUO~~) Since issuing the FY 2010 report, the IC CIO has closed one recommendation from the FY 2008 report. As noted below, the IC CIO still needs to address recommendation 1a to completely close out our FY 2008 recommendations. This recommendation resulted from Intelink's lack of a fully implemented and comprehensive information security program that is consistent with FISMA requirements. Intelink submitted their policies and procedures, periodic testing, Plan of Action and Milestones, and continuity of operations documentation. However, these documents do not meet the FISMA metric criteria.

Table 6: (U//~~FOUO~~) Status of FY 2008 FISMA Recommendations

Recommendation	MSD	IC CIO
1a. (U) The CIO should complete a documented comprehensive information security program consistent with FISMA requirements that includes the following elements: 1) periodic risk assessments, 2) policies and procedures based on risk assessments, 3) plans for providing appropriate information security, 4) periodic testing and evaluation of the information security policies and procedures, 5) a process for developing a plan of action, and 6) plans and procedures for developing continuity of operations for information systems. ²⁵	N/A	Open
1b. (U) CIO to establish milestones and complete strategic plans and programs and finalize system inventories.	N/A	Closed
1c. (U) CIO develop information security strategic plans that define the following for its information security program: 1) Clear and comprehensive mission, vision, goals, and objectives and how they relate to agency mission, 2) High level plan for achieving information security goals and objectives, including short and mid-term objectives to be used throughout the life of this plan to manage progress toward successfully fulfilling the identified objectives, and 3) Performance measures to continuously monitor accomplishment of identified goals and objectives and their progress toward stated targets.	Closed	Closed
1d. (U) The CIO should establish milestones for completion of the information security strategic plans.	Closed	Closed

²⁵ (U//~~FOUO~~) CIO is now referred to as IC CIO.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation	MSD	IC CIO
2a. (U) The CIO, in coordination with D/DMS, to establish a roadmap to identify the inventory of systems that are the ODNI responsibility and those that are IC-wide responsibility and establish a timeframe for completion of the roadmap. ²⁶	Closed	Closed
3a. (U) D/DMS to designate a senior agency official responsible for security of ODNI information and information systems whether ODNI owned or operated by another agency or by a contractor on behalf of ODNI.	Closed	N/A
3b. (U) D/DMS to complete a documented comprehensive information security program consistent with FISMA requirements that includes the following elements: 1) periodic risk assessments, 2) policies and procedures based on risk assessments, 3) plans for providing appropriate information security, 4) periodic testing and evaluation of the information security policies and procedures, 5) a process for developing a plan of action, and 6) plans and procedures for developing continuity of operations for information systems.	Closed	N/A
3c. (U) D/DMS to establish milestones for completion of the information security program.	Closed	N/A
3d. (U) D/DMS develop information security strategic plans that define the following for its information security program: 1) clear and comprehensive mission, vision, goals, and objectives and how they relate to agency mission, 2) high level plan for achieving information security goals and objectives, including short and mid-term objectives to be used throughout the life of this plan to manage progress toward successfully fulfilling the identified objectives, and 3) performance measures to continuously monitor accomplishment of identified goals and objectives and their progress toward stated targets.	Closed	N/A
3e. (U) D/DMS to establish milestones for completion of the information security strategic plans	Closed	N/A

Source: ODNI OIG review of MSD and Intelink documentation.

(U) Follow-Up on FY 2009 FISMA Recommendations

(U//~~FOUO~~) As mentioned earlier, since issuing the FY 2010 FISMA report, the ODNI has closed a total of 40 recommendations from our FY 2008, FY 2009, and FY 2010 FISMA reports. Eighteen (MSD closed 13 and IC CIO closed 5) of these recommendations were from the FY 2009 FISMA report and the implementation of these recommendations has improved the accuracy of the ODNI's system inventories and enhanced the plan of action and milestone process at the ODNI.

²⁶ (U//~~FOUO~~) D/DMS is now referred to as D/MSD.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U//~~FOUO~~) Nine recommendations from the OIG's FY 2009 FISMA report remain open. 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 in IC agencies given their respective missions. Without adequately addressing security concerns, the ODNI could leave its systems vulnerable to attacks.

(U//~~FOUO~~) Table 7 identifies the recommendations made to MSD and Intelink in the ODNI OIG's FY 2009 annual FISMA report and the status of their implementation.

Table 7: (U//~~FOUO~~) Status of FY 2009 FISMA Recommendations

Recommendation	MSD	IC CIO
1.1. a. (U// FOUO) Develop and maintain an accurate inventory of systems.	Closed	Open
1.1. b (U// FOUO) Determine ownership of the 7 unidentified systems.	Closed	Closed
1.1.c (U// FOUO) Make systems additions, deletions, or adjustments of the IC IT Registry in a timely manner	Closed	Open
1.2. (U// FOUO) Reconcile the systems' inventories with the IC IT Registry, at a minimum, on a quarterly basis	Open	Open
2.0. (U// FOUO) ADNI/CIO will develop a certification and accreditation strategy including a schedule (plan of action and milestones) for reaccrediting the cited systems and update this information in the IC Registry and the Director of the Mission Support Center will establish current certifications and accreditations for all systems identified under their ownership and update this information in the IC Registry.	Closed	Open
3. 0.a. (U// FOUO) Perform security tests on systems that currently have security tests greater than 1-year old.	Closed	Open
3. 0.b. (U// FOUO) Perform annual security tests on systems with a protection level greater than PL 1.	Closed	Open
4. 0.a. (U// FOUO) Establish a plan for performing contingency plan tests on systems whose contingency plan tests are greater than a year old and establish a designated period for future contingency plan tests.	Closed	Open
4. 0.b. (U// FOUO) Perform contingency plan tests on all systems with an availability rating of high.	Closed	Open
4. 0.c. (U// FOUO) Assign availability ratings to all ODNI systems on the IC Registry.	Closed	Closed

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation	MSD	IC CIO
5.0. a. (U// FOUO) Develop a uniform written plan of action and milestone process for the ODNI.	Closed	Closed
5.0.b. (U// FOUO) Revise their plan of action and milestone lists to include dates when items are placed on the lists, projected milestone dates, and actual completion dates so that progress on the actions can be monitored.	Closed	Closed
5.0.c. (U// FOUO) Review existing plan of action and milestone lists and determine which items can be easily remedied so they can be closed.	Closed	Closed
6.1 (U// FOUO) Jointly develop an ODNI configuration management policy <i>(Note: Because of changes to FISMA metrics for FY 2010, this recommendation is no longer appropriate. This report makes recommendations based on FY 2010 FISMA metrics).</i>	Closed	Closed
6.2. a. (U// FOUO) MSC and IECC should adopt and implement Federal Desktop Core Configuration (FDCC) standard configurations and document deviations and security control deficiencies on desktops directly controlled by ODNI.	Closed	N/A
6.2. b. (U// FOUO) Implement Federal Desktop Core Configuration security settings into all Windows XP™ and Vista™ desktops directly controlled by the ODNI.	Closed	N/A
7.0 (U// FOUO) Develop an incident reporting policy.	Closed	Closed
8.1. a. (U// FOUO) Designate personnel who have significant responsibilities for information security.	Closed	Closed
8.1. b. (U// FOUO) Develop an ODNI pilot training program and plan strategy to provide the designated personnel with training commensurate with their roles.	Closed	Closed
8.2 (U// FOUO) While accommodating ongoing operations and allowing time for contract modifications, ensure contracts specify that personnel who have significant responsibilities for information security receive training commensurate with their roles.	Closed	Closed
9.0 (U// FOUO) Fully implement all recommendations in the FY 2008 FISMA report.	Closed	Closed

Source: ODNI OIG review of MSD and Intelink documentation.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~**(U) Follow-Up on FY 2010 FISMA Recommendations**

(U//~~FOUO~~) Since issuing the FY 2010 FISMA report, the ODNI closed a total of 21 (MSD closed 15 and IC CIO closed 6) recommendations from our FY 2010 FISMA report. These recommendations were designed to reduce the vulnerability of ODNI systems to attack and compromise of critical information. Implementation of these recommendations has improved the accuracy of the ODNI's system inventories, clarified responsibilities for IT security, strengthened the ODNI's incident response and reporting program, and facilitated the planning and performance of contingency plan tests on IT systems.

(U//~~FOUO~~) Eleven recommendations from the OIG's FY 2010 FISMA report remain open. The IG FISMA review serves as an independent assessment to determine if the agency is utilizing a risk-based approach for their information security programs and systems that support the mission of the agency. Failure to address security concerns could leave agency systems vulnerable to attacks which are becoming increasingly more worrisome with terrorists potential ability to commit cyber warfare.

(U//~~FOUO~~) Table 8 identifies the recommendations made to MSD and Intelink in the ODNI OIG's FY 2010 annual FISMA report and the status of their implementation.

Table 8: (U//~~FOUO~~) Status of FY 2010 FISMA Recommendations

Recommendation	MSD	IC CIO
1.1. a (U// FOUO) Assign responsibility for timely updating and reconciling D/MSD and IC IT Registry system inventories.	Closed	N/A
1.1.b (U// FOUO) Reconcile MSD 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. Repeats 2009 Recommendations 1.1 and 1.2, due to be completed in January 2010.	Open	N/A
1.2. a (U// FOUO) Assign responsibility for timely updating and reconciling IECC and IC IT Registry system inventories. Repeats 2009 Recommendations 1.1 and 1.2, due to be completed in January 2010.	N/A	Closed
1.2.b (U// FOUO) Reconcile IECC 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. Repeats 2009 Recommendations 1.1 and 1.2, due to be completed in January 2010.	N/A	Open
2.1 (U// FOUO) Develop a schedule to test each information system with a PL 2 or higher within the next 12 months.	Closed	N/A

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation	MSD	IC CIO
2.2 (U// FOUO) Develop a schedule to test each information system with a PL 2 or higher within the next 12 months.	N/A	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.	Closed	N/A
2.4. a (U// FOUO) Perform security tests on systems that currently have security tests that are greater than 1-year old.	N/A	Open
2.4. b (U// FOUO) Perform annual security tests on systems with a PL greater than 1 within 12 months of their accreditation date or the date of last testing.	N/A	Open
3.1 (U// FOUO) Develop a certification and accreditation strategy including a schedule for accrediting its systems (systems should be certified and accredited within 12 months and the IC IT Registry updated accordingly). (U// FOUO) Repeats 2009 Recommendation 2.0, due to be completed in January 2010.	Closed	N/A
3.2 (U// FOUO) Ensure that the two systems currently operating without C&As receive their C&As. (U// FOUO) Repeats 2009 Recommendation 2.0, due to be completed in January 2010.	Closed	N/A
3.3 (U// FOUO) Develop a certification and accreditation strategy including a schedule for accrediting its systems (systems should be certified and accredited within 12 months and the IC IT Registry updated accordingly.) (U// FOUO) Repeats 2009 Recommendation 2.0, due to be completed in January 2010.	N/A	Open
4.1. a (U// FOUO) Revise the security configuration management oversight program for its systems that includes OMB's FY 2010 FISMA requirements.	Closed	N/A
4.1. b (U// FOUO) Revise its Service agreement with ISG to clarify ISG and MSC responsibilities for security.	Closed	N/A
4.1. c (U// FOUO) Establish responsibility for those CM functions that MSC will not include in the Service Agreement with ISG.	Closed	N/A
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.	Closed	N/A
4.2. a (U// FOUO) Establish a security configuration management program for its systems that meets OMB's FY 2010 FISMA requirements.	N/A	Closed
4.2. b (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.	N/A	Open

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation	MSD	IC CIO
5.1.a (U// FOUO) Revise and update the incident response and reporting program to include OMB's expectations for comprehensive analysis, validation, documentation, and resolution of incidents in a timely manner and timely reporting of incident data to appropriate authorities.	Closed	N/A
5.1.b (U// FOUO) Amend the Service Agreement with ISG to explicitly include requirements delineating specific roles and responsibilities that ISG will perform in assisting with the incident response and reporting functions; alternatively, MSC should institute measures that address incident response and reporting functions required by OMB.	Closed	N/A
5.2. a (U// FOUO) Finalize its draft Intelink Incident Response Plan and ensure that it meets or exceeds all requirements established by OMB and FISMA.	N/A	Closed
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.	N/A	Closed
6.1 (U// FOUO) Revise the current POA&M process to incorporate OMB's FY 2010 FISMA metrics into MSC's written POA&M program.	Closed	N/A
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.	N/A	Closed
7.1 (U// FOUO) Establish and document a continuous monitoring program incorporating all of OMB's requirements.	Closed	N/A
7.2 (U// FOUO) Establish and document a continuous monitoring program incorporating all of the OMB requirements.	N/A	Open
8.1. a (U// FOUO) Complete a contingency plan program including, at a minimum, the areas outlined in the OMB FY 2010 FISMA metrics.	Closed	N/A
8.1. b (U// FOUO) Complete contingency plans for all systems with availability level of concern ratings of medium or greater.	Closed	N/A
8.2. a (U// FOUO) Establish a contingency plan program including, at a minimum, the areas outlined in the OMB FY 2010 FISMA metrics.	N/A	Open
8.2.b (U// FOUO) Establish a plan for performing contingency plan tests on systems whose contingency plans are greater than 1-year old and establish a schedule for future contingency plan tests.	N/A	Open
8.2. c (U// FOUO) Perform contingency plan tests on all systems with availability ratings of high.	N/A	Open

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation	MSD	IC CIO
8.2. d (U// FOUO) Establish contingency plans for all systems with availability ratings of medium or greater.	N/A	Open

Source: ODNI OIG review of MSD and Intelink documentation.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~**(U) Annex A: List of Acronyms**

ATO	Approval to Operate
C&A	Certification and Accreditation
CIA	Central Intelligence Agency
CIGIE	Council of the Inspector General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CNSS	Committee on National Security Systems
D/MSD	Director – Mission Support Division
DCID	Director of Central Intelligence Directive
DNI	Director of National Intelligence
FAEC	Federal Audit Executive Council
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GCS	Global Communication Services
IATT	Interim Approval to Operate
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICIA	Intelligence Community Information Assurance
IC-IRC	Intelligence Community Incident Response Center
IC IT Registry	Intelligence Community Information Technology Registry
ICS	Intelligence Community Standard
ICD	Intelligence Community Directive
Intelink	Intelligence Community (IC) Enterprise Collaboration Center
ISG	Infrastructure Services Group
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
LOC	Levels of Concern
LX	Liberty Crossing
MOU	Memorandum of Understanding
MSD	Mission Support Division
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
OMB	Office of Management and Budget

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

PL	Protection Level
POA&M	Plan of Action and Milestones
SAOP	Senior Agency Official for Privacy
SOP	Standard Operating Procedures
SP	Special Publication
SSP	System Security Plan

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~**(U) Annex B: Matrix of ICIG FY 2011 FISMA Recommendations****Table 9: (U//~~FOUO~~) Status of FY 2011 FISMA Recommendations**

Recommendation	MSD	IC CIO
1.1. (U// FOUO) Perform an assessment of the network scans provided by the ISG at least annually to validate the MSD systems inventory	Open	N/A
1.2.a (U// FOUO) Assess systems inventory data by performing network scans at least annually to validate the Intelink systems inventory.	N/A	Open
1.2.b (U// FOUO) Develop and maintain an accurate inventory of systems.	N/A	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.	Closed	N/A
2.2. (U// FOUO) Perform security tests on systems that currently have security tests dates greater than one year.	N/A	Open
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.	Open	N/A
3.2 (U// FOUO) Update the certification and accreditation process and procedure documentation to ensure that it addresses the metric criteria, finalize all documentation, and indicate approval with a signature and date.	N/A	Open
3.3 (U// FOUO) Develop a C&A strategy including a schedule for reaccrediting its systems.	N/A	Open
4.1. a (U// FOUO) Revise the security configuration management oversight program for its systems that includes FY 2011 OIG FISMA metric requirements.	Closed	N/A
4.1. b (U// FOUO) Establish responsibility for those CM functions that MSD will not include in the Service Agreement with ISG.	Closed	N/A
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.	Closed	N/A
4.2.a (U// FOUO) Update the security configuration management policy and procedure documentation to ensure that it addresses the FY 11 FISMA metric criteria; finalize all documentation and indicate approval with a signature and date.	N/A	Open

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Recommendation	MSD	IC CIO
4.2.b (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.	N/A	Open
5.1 (U// FOUO) Establish a remote access program including at a minimum, the areas outlined in the FY 2011 OIG FISMA metrics	N/A	Open
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.	Open	N/A
6.2 (U// FOUO) Establish and document a continuous monitoring program incorporating all of the OMB requirements.	N/A	Open
7.1.a (U// FOUO) Establish a contingency plan program including, at minimum, the areas outlined in FY 2011 OIG FISMA metrics.	N/A	Open
7.1.b (U// FOUO) Establish a plan for performing contingency plan tests on systems whose contingency plan tests are greater than 1-year old and establish a schedule for future contingency plan tests.	N/A	Open
7.1. c (U// FOUO) Perform contingency plan tests on all systems with an availability rating of high.	N/A	Open
7.1. d (U// FOUO) Establish contingency plans for all systems with availability Level-of-Concern ratings of medium or greater.	N/A	Open

Source: ODNI OIG review of MSD and Intelink documentation.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

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

[REDACTED]												
[REDACTED]												
[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]		[REDACTED]		[REDACTED]		[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Certification and Accreditation Program

	<u>a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.
	2. Establishment of accreditation boundaries for agency information systems.
	3. Categorizes information systems.
	4. Applies applicable minimum baseline security controls,
	5. Assesses risks and tailors security control baseline for each system.
	6. Assessment of the management, operational, and technical security controls in the information system.
	7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.
	8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.
X	<u>b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Certification and accreditation policy is not fully developed.
	2. Certification and accreditation procedures are not fully developed or consistently implemented.
	3. Information systems are not properly categorized (FIPS 199/SP 800-60).
	4. Accreditation boundaries for agency information systems are not adequately defined.
	5. Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).
	6. Risk assessments are not adequately conducted (SP 800-30).
	7. Security control baselines are not adequately tailored to individual information systems (SP 800-30).
	8. Security plans do not adequately identify security requirements (SP 800-18).
	9. Inadequate process to assess security control effectiveness (SP800-53A).
	10. Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).
	11. Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).
	12. Other
	<u>c. The Agency has not established a certification and accreditation program.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Security Configuration Management Program

	<u>a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for configuration management.
	2. Standard baseline configurations.
	3. Scanning for compliance and vulnerabilities with baseline configurations.
	4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.
	5. Documented proposed or actual changes to the configuration settings.
	6. Process for the timely and secure installation of software patches.
X	<u>b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Configuration management policy is not fully developed.
	2. Configuration management procedures are not fully developed or consistently implemented.
	3. Software inventory is not complete (NIST 800-53: CM-8).
	4. Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).
	5. Hardware inventory is not complete (NIST 800-53: CM-8).
	6. Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
	7. Standard baseline configurations are not fully implemented (NIST 800-53: CM-h. FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.
	8. Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).
	9. Configuration related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2). j
	10. Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).
	11. Other
	12. Identify baselines reviewed:
	a. Software Name
	b. Software Version
	<u>c. The Agency has not established a security configuration management program.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Incident Response and Reporting Program

X	<p><u>a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u></p>
	1. Documented policies and procedures for responding and reporting to incidents.
	2. Comprehensive analysis, validation and documentation of incidents.
	3. When applicable, reports to US-CERT within established timeframes.
	4. When applicable, reports to law enforcement within established timeframes.
	5. Responds to and resolves incidents in a timely manner to minimize further damage.
	<p><u>b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u></p>
	1. Incident response and reporting policy is not fully developed.
	2. Incident response and reporting procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	4. Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	5. Incidents were not reported to law enforcement as required.
	6. Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	7. Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	8. There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	9. Other
	<p><u>c. The Agency has not established an incident response and reporting program.</u></p>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Security Training Program	
N/A	a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
	1. Documented policies and procedures for security awareness training.
	2. Documented policies and procedures for specialized training for users with significant information security responsibilities.
	3. Appropriate training content based on the organization and roles.
	4. Identification and tracking of all employees with login privileges that need security awareness training.
	5. Identification and tracking of employees without login privileges that require security awareness training.
	6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.
	b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:
	1. Security awareness training policy is not fully developed.
	2. Security awareness training procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Specialized security training policy is not fully developed.
	4. Specialized security training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).
	5. Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).
	6. Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
	7. Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
	8. Identification and tracking of employees with significant information security responsibilities is not adequate (SP 800-50, SP 800-53).
	9. Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).
	10. Less than 90% of employees with login privileges attended security awareness training in the past year.
	11. Less than 90% of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.
	12. Other
	c. The Agency has not established a security training program.
<p>Comments: ODNI follows CIA IA and Privileged user training. ISG tracks both and sends a report to MSD to identify those individuals noncompliant.</p>	

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Plans of Action and Milestones (POA&M) Program	
X	a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
	1. Documented policies and procedures for managing all known IT security weaknesses.
	2. Tracks, prioritizes and remediates weaknesses.
	3. Ensures remediation plans are effective for correcting weaknesses.
	4. Establishes and adheres to reasonable remediation dates.
	5. Ensures adequate resources are provided for correcting weaknesses.
	6. 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 POAM activities at least quarterly.
	b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:
	1. POA&M Policy is not fully developed.
	2. POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. POA&Ms do not include all known security weaknesses (OMB M-04-25).
	4. Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
	5. Initial date of security weaknesses are not tracked (OMB M-04-25).
	6. Security weaknesses are not appropriately prioritized (OMB M-04-25).
	7. Estimated remediation dates are not reasonable (OMB M-04-25).
	8. Initial target remediation dates are frequently missed (OMB M-04-25).
	9. POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
	10. Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).
	11. Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
	12. Other
	c. The Agency has not established a POA&M program.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Remote Access Program	
N/A	<u>a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.
	2. Protects against unauthorized connections or subversion of authorized connections.
	3. Users are uniquely identified and authenticated for all access.
	4. If applicable, multi-factor authentication is required for remote access.
	5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.
	6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.
	7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.
	<u>b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.</u>
	1. Remote access policy is not fully developed.
	2. Remote access procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).
	4. Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4).
	5. Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).
	6. Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).
	7. Agency has not identified all remote devices (NIST 800-46, Section 2.1).
	8. Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).
	9. Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46, Section 3.2).
	10. Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
	11. Remote access rules of behavior are not adequate (NIST 800-53, PL-4).
	12. Remote access user agreements are not adequate (NIST 800-46, Section 5.1, NIST 800-53, PS-6).
	13. Other
	<u>c. The Agency has not established a program for providing secure remote access.</u>
Comments: The ODNI/MSD does not have a need for a remote access program	

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Account and Identity Management Program

N/A	<u>a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for account and identity management.
	2. Identifies all users, including federal employees, contractors, and others who access Agency systems.
	3. Identifies when special access requirements (e.g., multifactor authentication) are necessary.
	4. If multi-factor authentication is in use, it is linked to the Agency's PIV program.
	5. Ensures that the users are granted access based on needs and separation of duties principles.
	6. Identifies devices that are attached to the network and distinguishes these devices from users.
	7. Ensures that accounts are terminated or deactivated once access is no longer required.
	<u>b. The Agency has established and is maintaining an account and identify management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Account management policy is not fully developed.
	2. Account management procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Active Directory is not properly implemented (NIST 800-53, AC-2).
	4. Other Non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).
	5. Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).
	6. Accounts are not properly issued to new users (NIST 800-53, AC-2).
	7. Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).
	8. Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).
	9 Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).
	10. Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	11. Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	12. Network devices are not properly authenticated (NIST 800-53, IA-3).
	13. Other
	<u>c. The Agency has not established an account and identity management program.</u>
Comments: Not Applicable at this time since MSD follows CIA policies and ISG manages the policy enforcement.	

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Continuous Monitoring Program

a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	
	1. Documented policies and procedures for continuous monitoring.
	2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.
	3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.
	4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.
X	b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:
	1. Continuous monitoring policy is not fully developed.
	2. Continuous monitoring procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).
	4. Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).
	5. The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).
	6. Other
c. The Agency has not established a continuous monitoring program.	

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Contingency Planning Program	
X	<p><u>a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u></p> <ol style="list-style-type: none"> 1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster. 2. The agency has performed an overall Business Impact Assessment. 3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures. 4. Testing of system specific contingency plans. 5. The documented business continuity and disaster recovery plans are ready for implementation. 6. Development of training, testing, and exercises (TT&E) approaches. 7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans. <p><u>b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u></p> <ol style="list-style-type: none"> 1. Contingency planning policy is not fully developed. 2. Contingency planning procedures are not fully developed, sufficiently detailed, or consistently implemented. 3. An overall business impact assessment has not been performed (NIST SP 800-34). 4. Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34). 5. A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34). 6. A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34). 7. System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53). 8. Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53). 9. Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST SP 800-53). 10. Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53). 11. Disaster recovery exercises were not successful revealed significant weaknesses in the contingency planning (NIST SP 800-34). 12. After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34). 13. Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). 14. Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53). 15. Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

	16. Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
	17. Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	18. Other
	<u>c. The Agency has not established a business continuity/disaster recovery program.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the MSD Agency Program to Oversee Contractor Systems	
N/A	<u>a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities and that the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.
	2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.
	3. The inventory identifies interfaces between these systems and Agency-operated systems.
	4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.
	5. The inventory, including interfaces, is updated at least annually.
	6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.
	<u>b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.
	2. Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed, sufficiently detailed, or consistently implemented.
	3. The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.
	4. The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.
	5. The inventory of contractor/entity operated systems, including interfaces, is not updated at least annually.
	6. Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., certification and accreditation requirements).
	7. Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., certifications and accreditation requirements).
	8. Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.
	9. Other
	<u>c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

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

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

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Certification and Accreditation Program

	a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
	1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.
	2. Establishment of accreditation boundaries for agency information systems.
	3. Categorizes information systems.
	4. Applies applicable minimum baseline security controls,
	5. Assesses risks and tailors security control baseline for each system.
	6. Assessment of the management, operational, and technical security controls in the information system.
	7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.
	8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.
X	b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:
	1. Certification and accreditation policy is not fully developed.
	2. Certification and accreditation procedures are not fully developed or consistently implemented.
	3. Information systems are not properly categorized (FIPS 199/SP 800-60).
	4. Accreditation boundaries for agency information systems are not adequately defined.
	5. Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).
	6. Risk assessments are not adequately conducted (SP 800-30).
	7. Security control baselines are not adequately tailored to individual information systems (SP 800-30).
	8. Security plans do not adequately identify security requirements (SP 800-18).
	9. Inadequate process to assess security control effectiveness (SP800-53A).
	10. Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).
	11. Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).
	12. Other
	c. The Agency has not established a certification and accreditation program.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Security Configuration Management Program

	<u>a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for configuration management.
	2. Standard baseline configurations.
	3. Scanning for compliance and vulnerabilities with baseline configurations.
	4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.
	5. Documented proposed or actual changes to the configuration settings.
	6. Process for the timely and secure installation of software patches.
X	<u>b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Configuration management policy is not fully developed.
	2. Configuration management procedures are not fully developed or consistently implemented.
	3. Software inventory is not complete (NIST 800-53: CM-8).
	4. Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).
	5. Hardware inventory is not complete (NIST 800-53: CM-8).
	6. Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
	7. Standard baseline configurations are not fully implemented (NIST 800-53: CM-h. FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.
	8. Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).
	9. Configuration related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2). j
	10. Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).
	11. Other
	12. Identify baselines reviewed: a. Software Name
	b. Software Version
	<u>c. The Agency has not established a security configuration management program.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Incident Response and Reporting Program

X	<p><u>a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u></p>
	1. Documented policies and procedures for responding and reporting to incidents.
	2. Comprehensive analysis, validation and documentation of incidents.
	3. When applicable, reports to US-CERT within established timeframes.
	4. When applicable, reports to law enforcement within established timeframes.
	5. Responds to and resolves incidents in a timely manner to minimize further damage.
	<p><u>b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u></p>
	1. Incident response and reporting policy is not fully developed.
	2. Incident response and reporting procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	4. Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	5. Incidents were not reported to law enforcement as required.
	6. Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	7. Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	8. There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	9. Other
	<p><u>c. The Agency has not established an incident response and reporting program.</u></p>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Security Training Program	
N/A	<p><u>a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u></p>
	1. Documented policies and procedures for security awareness training.
	2. Documented policies and procedures for specialized training for users with significant information security responsibilities.
	3. Appropriate training content based on the organization and roles.
	4. Identification and tracking of all employees with login privileges that need security awareness training.
	5. Identification and tracking of employees without login privileges that require security awareness training.
	6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.
	<p><u>b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u></p>
	1. Security awareness training policy is not fully developed.
	2. Security awareness training procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Specialized security training policy is not fully developed.
	4. Specialized security training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).
	5. Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).
	6. Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
	7. Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
	8. Identification and tracking of employees with significant information security responsibilities is not adequate (SP 800-50, SP 800-53).
	9. Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).
	10. Less than 90% of employees with login privileges attended security awareness training in the past year.
	11. Less than 90% of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.
	12. Other
	<p><u>c. The Agency has not established a security training program.</u></p>
<p>Comments: ODNI follows CIA IA and Privileged user training. ISG tracks both and sends a report to MSD (Intelink staff are included in this report) to identify those individuals noncompliant.</p>	

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Plans of Action and Milestones (POA&M) Program	
X	<p><u>a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u></p>
	1. Documented policies and procedures for managing all known IT security weaknesses.
	2. Tracks, prioritizes and remediates weaknesses.
	3. Ensures remediation plans are effective for correcting weaknesses.
	4. Establishes and adheres to reasonable remediation dates.
	5. Ensures adequate resources are provided for correcting weaknesses.
	6. 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 POAM activities at least quarterly.
	<p><u>b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u></p>
	1. POA&M Policy is not fully developed.
	2. POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. POA&Ms do not include all known security weaknesses (OMB M-04-25).
	4. Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
	5. Initial date of security weaknesses are not tracked (OMB M-04-25).
	6. Security weaknesses are not appropriately prioritized (OMB M-04-25).
	7. Estimated remediation dates are not reasonable (OMB M-04-25).
	8. Initial target remediation dates are frequently missed (OMB M-04-25).
	9. POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
	10. Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).
	11. Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
	12. Other
	<p><u>c. The Agency has not established a POA&M program.</u></p>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Remote Access Program

	<u>a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.
	2. Protects against unauthorized connections or subversion of authorized connections.
	3. Users are uniquely identified and authenticated for all access.
	4. If applicable, multi-factor authentication is required for remote access.
	5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.
	6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.
	7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.
	<u>b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.</u>
	1. Remote access policy is not fully developed.
	2. Remote access procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).
	4. Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4).
	5. Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).
	6. Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).
	7. Agency has not identified all remote devices (NIST 800-46, Section 2.1).
	8. Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).
	9. Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46, Section 3.2).
	10. Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
	11. Remote access rules of behavior are not adequate (NIST 800-53, PL-4).
	12. Remote access user agreements are not adequate (NIST 800-46, Section 5.1, NIST 800-53, PS-6).
	13. Other
X	<u>c. The Agency has not established a program for providing secure remote access.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Account and Identity Management Program

N/A	<p>a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p>
	1. Documented policies and procedures for account and identity management.
	2. Identifies all users, including federal employees, contractors, and others who access Agency systems.
	3. Identifies when special access requirements (e.g., multifactor authentication) are necessary.
	4. If multi-factor authentication is in use, it is linked to the Agency's PIV program.
	5. Ensures that the users are granted access based on needs and separation of duties principles.
	6. Identifies devices that are attached to the network and distinguishes these devices from users.
	7. Ensures that accounts are terminated or deactivated once access is no longer required.
	<p>b. The Agency has established and is maintaining an account and identify management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</p>
	1. Account management policy is not fully developed.
	2. Account management procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Active Directory is not properly implemented (NIST 800-53, AC-2).
	4. Other Non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).
	5. Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).
	6. Accounts are not properly issued to new users (NIST 800-53, AC-2).
	7. Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).
	8. Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).
	9 Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).
	10. Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	11. Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	12. Network devices are not properly authenticated (NIST 800-53, IA-3).
	13. Other
	<p>c. The Agency has not established an account and identity management program.</p>
<p>Comments: Not Applicable at this time since Intelink follows CIA policies and ISG manages the policy enforcement.</p>	

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Continuous Monitoring Program

	<u>a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for continuous monitoring.
	2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.
	3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.
	4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.
	<u>b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Continuous monitoring policy is not fully developed.
	2. Continuous monitoring procedures are not fully developed, sufficiently detailed, or consistently implemented.
	3. Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).
	4. Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).
	5. The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).
	6. Other
X	<u>c. The Agency has not established a continuous monitoring program.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Contingency Planning Program

a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.
2. The agency has performed an overall Business Impact Assessment.
3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.
4. Testing of system specific contingency plans.
5. The documented business continuity and disaster recovery plans are ready for implementation.
6. Development of training, testing, and exercises (TT&E) approaches.
7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:

1. Contingency planning policy is not fully developed.
2. Contingency planning procedures are not fully developed, sufficiently detailed, or consistently implemented.
3. An overall business impact assessment has not been performed (NIST SP 800-34).
4. Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).
5. A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).
6. A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).
7. System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).
8. Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).
9. Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST SP 800-53).
10. Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
11. Disaster recovery exercises were not successful revealed significant weaknesses in the contingency planning (NIST SP 800-34).
12. After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).
13. Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
14. Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
15. Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

	16. Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
	17. Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	18. Other
X	<u>c. The Agency has not established a business continuity/disaster recovery program.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Status of the Intelink Agency Program to Oversee Contractor Systems	
N/A	<u>a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</u>
	1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities and that the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.
	2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.
	3. The inventory identifies interfaces between these systems and Agency-operated systems.
	4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.
	5. The inventory, including interfaces, is updated at least annually.
	6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.
	<u>b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below. If b. checked above, check areas that need significant improvement:</u>
	1. Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.
	2. Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed, sufficiently detailed, or consistently implemented.
	3. The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.
	4. The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.
	5. The inventory of contractor/entity operated systems, including interfaces, is not updated at least annually.
	6. Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., certification and accreditation requirements).
	7. Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., certifications and accreditation requirements).
	8. Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.
	9. Other
	<u>c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.</u>

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

(U) Fiscal Year 2011 Independent Evaluation of ODNI Compliance with the Federal
Information Security Management Act of 2002

OIG Report No.: AUD-2012-003

~~SECRET//NOFORN~~