

Department of the Navy



Federal Information Security Management Act (FISMA) Guidance

March 2006

A handwritten signature in black ink, appearing to read "Robert J. Carey". The signature is written over a horizontal line.

ROBERT J. CAREY
Department of the Navy Deputy Chief Information Officer
(Policy and Integration) and
Department of the Navy Senior Information Assurance Official

EXECUTIVE SUMMARY

Information technology (IT) has significantly improved the Department of the Navy's (DON) operational efficiency, but the challenge of providing naval forces with secure methods of communication and information continues to grow. The Navy and the Marine Corps must be able to defend against increased threats from more sophisticated network intruders and cyber terrorists. The E-Government Act of 2002 addresses information assurance (IA) with its inclusive Federal Information Security Management Act (FISMA). FISMA is only a tool in a framework to gain and sustain information security while affording operational effectiveness. The purpose of this document is to provide guidance to DON commands as we all continue to improve the DON's IA posture as well as implement effective information security through FISMA compliance. The overall goal is to be proactive rather than reactive toward information and information system security.

This guidance document outlines four goals that the DON Chief Information Officer (CIO) uses to measure the degree to which the Department achieves its information security requirements. The DON FISMA Guidance applies a methodology that assesses current progress, establishes objectives, identifies required actions, and formulates performance metrics, to evaluate progress made toward each goal's objectives.

Goal	Area	Objectives
1	Risk Analysis and Management Oversight	Maintain information assurance and submit annual FISMA Report. Ensure compliance with Federal, Department of Defense (DoD), and DON policies and procedures. Ensure risk is analyzed and managed by using Certification and Accreditation (C&A) processes for systems and networks. Maintain current C&A status in the DoD Information Technology Portfolio Registry - DON (DITPR-DON) for systems, and in the DISA Connection Approval Process (CAP) database for networks. Achieve 100% C&A rate within the DON for full or interim accreditation, and at least 90% full accreditation.
2	Incident Response	Ensure effective procedures are in place for preventing, mitigating, and reporting security threats and incidents.
3	Awareness and Training	Ensure adequate IA awareness and training for the DON personnel and provide appropriate training to individuals with established IA roles.
4	Capital Planning	Ensure that IA plays a prominent role in the capital planning cycle and that newly acquired products and systems meet the DON guidance. Acquisition planning contains IA as a keystone to success.

In achieving these goals, a system of metrics to provide a measure of success has been developed and will be enhanced as opportunities and experience dictate. These quantifiable IA metrics are based on IT security performance goals and objectives, feasible to measure, repeatable, useful for tracking performance and directing resources, and able to identify relevant performance trends over time. Metrics analysis is used to apply lessons learned, improve the effectiveness of existing security controls, and plan future controls to meet new security requirements as they occur. An initial set of metrics is included within this document. The process will take time to

evolve before becoming fully mature. Results produced by the initial metrics process will open the door to further improvements in metrics identification and collection.

The DON FISMA Annual Report, submitted to the DoD CIO, provides a summary of the state of information assurance to the DON leadership and the Office of the Secretary of Defense (OSD). From each of the defense agencies' reports, the DoD CIO submits a composite DoD FISMA Report to the Office of Management and Budget (OMB) and to Congress. The FISMA report contains three major sections: Information Assurance, Privacy, and the DoD Inspector General assessment. The report summarizes information security parameters, taken from the DITPR-DON and from the reports submitted by the defense agencies, including the Military Departments (MILDEPs). Besides being a major report on the state of information assurance and privacy within the agency or MILDEP, Congress and OMB may make major funding decisions based on the results. The ability to spend funds on programs may very well be dependent upon achieving full accreditation of program systems.

Hence the importance of adherence to FISMA requirements and of the FISMA Report cannot be overemphasized.

TABLE OF CONTENTS

1. INTRODUCTION.....	1
2. PURPOSE	2
3. SCOPE	2
4. ROLES AND RESPONSIBILITIES	2
5. FISMA REPORT.....	4
6. METRICS	4
7. ANALYSIS OF GOALS.....	10
8. CONCLUSION.....	15

APPENDIX A: Metrics Matrix

APPENDIX B: Plan of Action and Milestones (POA&M) Process

APPENDIX C: Acronyms

1. INTRODUCTION

Information technology (IT) has significantly improved the Department of the Navy's (DON) operational efficiency, but the challenge of providing naval forces with secure methods of communication and information continues to grow. The Navy and the Marine Corps must be able to detect, react to, and prevent or mitigate increased threats from more sophisticated network intruders and cyber terrorists. Compromise of information or denial of access to information resources would have major, detrimental effects on the ability of the Navy and the Marine Corps to fulfill their missions. Thus, securing our information using information assurance (IA) strategies is a top priority for the DON.

The Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002 (Public Law 107-347), addresses program management and evaluation aspects of information assurance. The FISMA legislation requires Federal agencies to:

- Develop and implement an agency-wide information security program and ensure the plan is practiced throughout the life cycle of each system.
- Conduct annual reviews of the agency-wide information security program, including risk assessments, tests, and evaluations.
- Develop and implement policies and procedures for an incident response, detection, and reporting capability.
- Ensure that information security plays an integral role in the IT budget and capital planning process.
- Train and oversee personnel with significant responsibilities for information security.
- Submit an annual report providing status of information security within the Department.

The overarching goal of the Department of the Navy Chief Information Officer (DON CIO) is to secure the Department's information assets, balancing the need for security with the primary objective of meeting operational requirements. The ability to spend funds on programs may very well be dependent upon achieving full certification and accreditation (C&A) of program systems.

The DON CIO makes a concerted effort to reassess its policies and procedures regularly. The Office of Management and Budget (OMB), the Office of the Secretary of Defense (OSD), and the DON have previously identified findings that influence the direction taken by information assurance and FISMA compliance. In its Fiscal Year 2001 report to Congress on the status of information security reform within the Federal Government, OMB cited the need to:

- Increase senior management's visibility of information security issues.
- Improve security awareness and training.
- Integrate security into IT capital planning.
- Detect, share, and report security vulnerability information.
- Establish a performance measures program.

- Ensure secure contractor services.

2. PURPOSE

The purposes of this document are to lay a foundation for improving the DON's information assurance posture and outline courses of action to comply with FISMA. The DON FISMA Guidance supports and complements current Secretary of the Navy IA Policy (SECNAVINST 5239.3A). This plan bolsters established policies and procedures to ensure FISMA compliance and improve the DON's overall IA posture.

3. SCOPE

The DON FISMA Guidance applies to:

- *Senior Leaders.* DON commanders, program managers, and civilian heads of organizations. This plan emphasizes the important roles that leadership plays in the overall information security posture of the DON.
- *Individuals.* All DON personnel, regardless of rank, grade, title, or position, who are responsible for safeguarding information and information systems, and for following established policies and guidance.
- *Supporting Organizations.* Commands such as the Naval Audit Service, Naval Inspector General, Navy Network Warfare Command (NNWC), Navy Information Operations Command (NIOC), and the Marine Corps Network Operations and Security Command (MCNOSC) who all play essential roles in the DON IA program.
- *Contractors.* FISMA applies to vendor organizations participating in support of the Department of the Navy.

4. ROLES AND RESPONSIBILITIES

The Department of the Navy Chief Information Officer (DON CIO)

The DON CIO is responsible for establishing overall policy, strategic direction of the DON IA, and coordination of FISMA efforts. Tasks include:

- Enforce FISMA compliance.
- Recommend budget adjustments to Assistant Secretary of the Navy, Financial Management and Budgeting (ASN-FMB) for systems failing to comply with IA requirements (e.g., continued lack of system accreditation).
- Compile and assess FISMA Report data required by OMB and DoD CIO FISMA guidance, and as reported by the Navy and Marine Corps.
- Prepare and submit a composite annual DON FISMA report to the DoD CIO.
- Monitor the currency and accuracy of DoD Information Technology Portfolio Registry - DON (DITPR-DON) and the DoD DITPR registries and update the DoD DITPR registry at least quarterly and more often as required.

- Actively promote IA metrics as an essential means of assessing IT security performance.
- Coordinate with the Naval Audit Service for annual assessments required by FISMA.
- Coordinate and align Designated Approving Authority (DAA) procedures for achieving certification and accreditation.
- Maintain the DON FISMA Guidance.

Assistant Secretary of the Navy, Research, Development, and Acquisition (ASN-RDA)

- Ensure IA is built into all phases of program acquisition, in accordance with DoD and SECNAV acquisition directives.

Chief of Naval Operations, Commandant of the Marine Corps, and Secretary of the Navy Assistant for Administration (AAUSN)

These officials are responsible for establishing and executing overall IA programs within their realm, and the carrying out of FISMA requirements. The respective DON Deputy CIO and AAUSN coordinate with the DON CIO in these requirements.

- Establish and execute an IA program that meets or exceeds all requirements.
- Ensure that IA considerations are part of the requirements for information systems.
- Ensure risk management guidelines contained in FISMA legislation are incorporated in their respective systems, e.g., certification and accreditation accomplished, security and contingency plans developed and tested, life-cycle security costs identified, training status maintained, and so on.
- Monitor and validate the DITPR-DON and the Defense Information Security Agency (DISA) Connection Approval Process (CAP) databases.
- Provide DON CIO with appropriate performance metrics at the rate identified in Appendix A, and with other notable IA items as appropriate.
- Comply with or recommend changes to Appendix A and the metrics process.
- Carry out a Plan of Actions and Milestones (POA&M) process as discussed in Appendix B of this guidance.
- Designate and approve DAAs in accordance with current requirements.
- Coordinate the collection of FISMA data required by DON CIO FISMA guidance.
- Compile and assess FISMA Report data required by DON CIO FISMA guidance.
- Prepare and submit to DON CIO the data input for the annual FISMA Report.

Commanders of DON Organizations and Program Managers

- Carry out an effective information security program, in accordance with applicable directives issued by SECNAV, OSD, and Commander Joint Chiefs of Staff. The program must include as a minimum:
 - Periodic (at least annual) review, evaluation, and testing of system security, security controls, and continuity of operations plans.
 - Current C&A of systems and networks, with emphasis on full accreditation.
 - Annual IA Awareness training and specialized training for IT personnel, as required.
- Ensure that DITPR-DON and the DISA CAP databases are maintained accurately and completely for all DON systems and networks.

5. FISMA REPORT

The DON CIO submits an annual report to the DoD CIO, generally during July, regarding the status of information security within the Department. OSD provides guidance to the Military Departments (MILDEPs) and Components for this report, based on guidance provided by OMB. OSD receives reports from each of the Defense Agencies and MILDEPs, and in turn submits a composite FISMA report to OMB. OMB then submits a composite Federal Government FISMA Report to Congress, which forms the basis for a Congressional annual “grade” for information security within the Federal Government, and may form the basis for future funding decisions.

The DoD FISMA Report is comprised of three main sections: Information Security (including training), Privacy, and the DoD Inspector General (DoD-IG) assessment. The DON CIO submits the Information Security FISMA Report directly to the DoD CIO, and an input for Privacy to the DON Privacy Officer. The DoD-IG submits its report directly to the DoD CIO for inclusion in the OSD FISMA Report. The DoD-IG report incorporates audits from the various audit agencies and inspectors general into one composite overview.

The FISMA report generally consists of system security and privacy metrics taken from DITPR-DON, plus IA training data, network penetration data, system configuration management, POA&M status, and descriptive information as required by OMB and OSD. DON CIO coordinates report generation with the Navy and Marine Corps IA organizations, primarily the DON Deputy CIOs for the Navy and Marine Corps and AAUSN. OMB, OSD, and DON CIO annually issue detailed guidance for preparing the next report.

6. METRICS

IA metrics quantify the level of implementation of security controls, and help identify possible actions for improvement. Goals and objectives from DON guidance, OSD guidance, and Federal guidance and legislation are identified and prioritized during metrics development, to ensure that the measurable aspects of security performance correspond to operational priorities. Metrics also provide a convenient and timely means of monitoring the state of information security within the Department.

Metrics must yield quantifiable information to enable comparison, analysis, and tracking of changes using the same points of reference. Data required for calculating metrics must be readily obtainable, and the process under consideration needs to be measurable. The metrics process will take time to evolve before full maturation. Time and experience are necessary to establish data sources, develop tools to collect data, create baselines, and allow staff to become proficient in collecting data. Results produced by the metrics process will enable further improvements in metrics identification and collection, with a goal to improve awareness within the DON, and especially within DON leaders, to the need for information assurance.

Figure 1 illustrates how a metrics program should mature. There are five levels in National Institute of Science and Technology (NIST) Publication 800-26, *Security Self-Assessment for Information Technology System*, used to describe the maturity level of a metrics program that would be helpful to the DON. The levels are:

- Level 1 – Control objective documented in a security policy.
- Level 2 – Security controls documented as procedures.
- Level 3 – Procedures implemented.
- Level 4 – Procedures and security controls tested and reviewed.
- Level 5 – Procedures and security controls fully integrated into a comprehensive process.

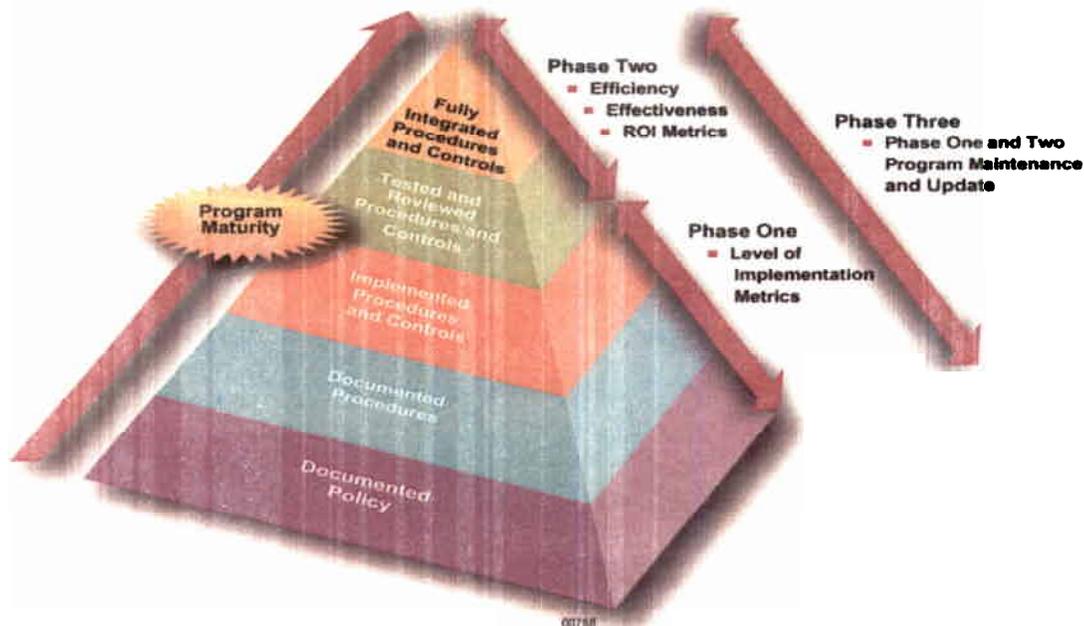


Figure 1. Phased Evolution of a Metrics Process

The IA metrics process emphasizes consistent periodic metrics data analysis. The results of this analysis are used to apply lessons learned, improve the effectiveness of existing security controls, and plan future controls to meet new security requirements as they occur. The Metrics Matrix, Appendix A, lists the specific data to be accumulated.

The DON IA metrics will be used to:

- Enable senior management to identify information security shortfalls.
- Identify goal areas that require additional support/resources.
- Facilitate improvement by establishing objective standards.
- Identify areas where behavior and accountability may need changing.
- Track trends in the overall DON IA posture.

The NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, provides a method of metrics development and implementation consisting of the following steps:

1. **Metrics Development:** Develop measurement tools.
2. **Data Collection and Storage:** Collect data from identified sources.
3. **Analysis and Reporting:** Establish performance baselines used to evaluate progress.
4. **Corrective Actions and Continuous Impact:** Identify concrete actions necessary to achieve the objective and to continuously evaluate progress.

Figure 2, taken from the NIST guidance, depicts these steps as part on an ongoing metrics program. Metrics, however, are collected more often than annually, as specified in Appendix A.

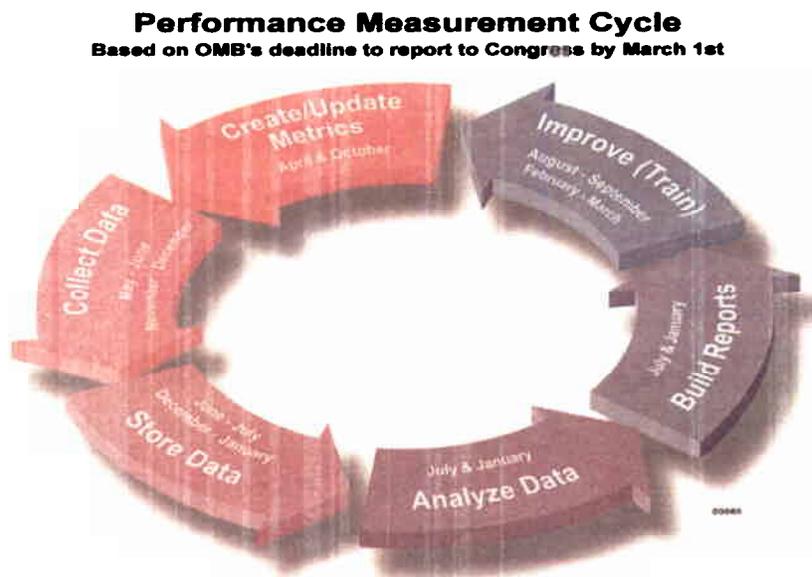


Figure 2. Semiannual Performance Measurement Cycle

Step 1: Metrics Development. This step involves activities that are key for establishing a comprehensive IA metrics process, including metrics identification, definition, development, and selection activities, and developing a metrics process implementation plan. After the metrics have been identified, the metric process will define specific implementation steps, including:

- Metrics roles and responsibilities.
- Details of coordination between DON CIO, the Navy, and the Marine Corps to ensure the metrics are streamlined and non-obtrusive.
- Metrics summary reporting formats.

Step 2: Data Collection and Storage. The metrics process will identify the metrics' sources. Initial data collection efforts will focus on using readily available sources to provide information for the calculations. Data collection will come from the following sources:

- DITPR-DON.
- DADMS – DADMS is a web-enabled registry of Navy and Marine Corps systems and applications, and their associated data structures and data exchange formats. It supports DON in the reduction of legacy applications and databases, the development of standard application, databases, and data elements, and the construction and maintenance of Functional and Enterprise architectures. DADMS contains DITPR-DON.
- Other existing DON sources.
- Supplemental sources to be developed.

Step 3: Analysis and Reporting. This step of the process involves activities that are essential for ensuring that the collected metrics are used to gain an understanding of system security and to identify appropriate improvement actions. This step includes the following activities:

- Conduct gap analysis to determine if the metrics address IA program goals.
- Identify causes of poor performance in meeting IA program goals.
- Identify any other IA program goal areas requiring attention.

Identifying poor performance is tightly linked to the causation factors found during individual metrics collection. For example, determining that the percentage of approved security plans is unacceptably low would not be helpful in determining how to correct the problem. To determine the cause of low compliance, information will need to be collected regarding the reasons for low percentages (e.g., lack of guidance, insufficient expertise, or conflicting priorities). Once this information is collected and compiled, corrective actions can be targeted.

Step 4: Corrective Actions and Continuous Improvement, including:

- Determine range of corrective actions. Based on the results and causation factors, identify corrective actions that could be applied to the problem. Corrective actions may include changing system configurations; training security staff, system administrator staff, or regular users; purchasing security tools; changing system architecture; establishing new processes and procedures; and updating security policies.
- Prioritize corrective actions based on overall risk mitigation goals. There may be several corrective actions applicable to a single performance issue. Applicable corrective actions should be prioritized according to impact, and a cost determination made.
- Select most appropriate corrective actions.

The final part of the process involves implementing corrective actions in technical, management, and operational areas of security controls. After corrective actions are applied, the cycle completes itself and restarts with subsequent data collection and analysis.

Iterative data collection, analysis, and reporting will help track progress of corrective actions, measure improvement, and identify the need for further improvement in the overall metrics process. The iterative nature of the cycle ensures that progress is monitored and corrective actions ultimately affect system security control implementation in a positive way. Performance measurements will ensure that if corrective actions are not implemented as planned, or if their effect is not as desired, mid-course corrections can be made, internally to the organization, therefore avoiding problems being discovered during external audits, certification and accreditation efforts, or other similar activities.

The specific metrics to be accumulated are listed in Appendix A.

IA Program Goals

The goals of the metrics process are categorized as follows:

- **Risk Analysis and Management Oversight.** The FISMA legislation centerpiece is risk management – assessing risk and magnitude of possible harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. The DON goal is to maintain between 90-100 percent of DON systems fully certified and accredited with a final Authority to Operate (ATO), and 100% of DON systems certified and accredited with either an ATO or an Interim Authority to Operate (IATO). Another goal is to address and minimize security weaknesses in DON systems and networks, and in audit reports.
 - A primary focus of risk management is the C&A of DON IT systems. In addition, other security measures are important, e.g., security and continuity of operations plans, as well as the exercising of these plans. The metrics in this category center on an adequate risk management program, and are reported in the annual FISMA report.
 - National Security Agency (NSA) sponsored teams assist commands and organizations in improving their IA posture. Red Teams conduct unannounced testing, Blue Teams provide technical assist visits upon request, Green Teams test the system and report to the requesting organization, and White Teams review the administration of information security. These teams provide great value in assessing and improving information assurance throughout the DON.
 - A material weakness document, submitted by DON CIO to the Assistant Secretary of the Navy for Financial Management and Comptroller (ASN (FM&C)), focuses attention on significant deficiencies in information assurance. A POA&M in the material weakness lays out the groundwork for correction of the weakness.
- **Designated Approving Authority (DAA) Coordination.** The DON goal is to align activities of the Department of the Navy DAA, the Navy DAAs, and the Marine Corps DAAs in order to have consistent policies that are well known to DON Commanders.

- **Incident Response.** The DON goal is ultimate protection of our systems and networks – to block all penetrations, be 100 percent in Information Assurance Vulnerability Alert (IAVA) compliance, and to conduct at least annual vulnerability assessments and penetration testing.
 - Tracking incidents to Navy and Marine Corps systems provides a measure for the success of security measures and the effectiveness of the Information Assurance Vulnerability Management (IAVM) process.
 - The IAVM process provides positive control of the vulnerability notification and corrective action process within DoD. The IAVM process helps to protect systems and networks from unauthorized access and attacks. The process is managed and carefully tracked by the DON IT protection organizations and by the Office of the Secretary of Defense (OSD).
 - Vulnerability assessments and penetration testing are accomplished to check the effectiveness of network and system defense-in-depth. A fully effective way of determining total DON systems protection would be to develop mapping of system location to sites, e.g., Defense Enterprise Computing Centers, MCNOSC, etc. Until this mapping is accomplished, percentage data will have to be estimated.
- **Awareness and Training.** The DON goals are to ensure 100% IA awareness training for all DON personnel (military, civilian, and on-site contractors), and up-to-date training and certification for all personnel with privileged access to DON networks.
 - DON IA policy, DoD IA policy, and FISMA require IA training in several categories including training for system users on an annual basis, specific training for system administrators, and Designated Approving Authority (DAA) training. These metrics require statistics on these categories of personnel and their training status.
 - The standards for IA training are contained in DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, and its associated DoD Manual 8570.01M, *Information Assurance Workforce Improvement Program*.
- **Capital Planning.** The DON goals in this area are to have no DON systems on the OMB watch list for security, maintain full accreditation for DON systems, ensure Clinger-Cohen requirements are satisfied for major acquisitions, and ensure all acquisitions of IA products certified by the National Information Assurance Partnership (NIAP) process.
 - Capital Asset Plans and Justifications (Exhibits 300) are submitted for major acquisition programs in accordance with OMB requirements. The security section of the Exhibit 300 is particularly important and must receive a high "grade" (4 out of a possible 5) if the plan is to be considered satisfactory. Metrics help the DON to better track financial plans. In addition, the annual FISMA report requires this metric data.
 - OMB requires that Exhibits 300 for systems that are not yet fully accredited include a POA&M for completion of system accreditation. OMB places systems without full accreditation and without a POA&M in an "at risk" category, which may have future funding implications.
 - SECNAVINST 5000.2C, "Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System," requires IA

Strategies be submitted for Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS). DON CIO reviews and approves these IA Strategies before the program can proceed to the next milestone.

- DoDI 8500.2, "Information Assurance Implementation," requires that after 1 July 2002, IA and IA-related IT products must be certified by the NIAP process, as discussed in the National Security Telecommunications Information Systems Security Policy (NSTISSP) Policy 11.

IA Dashboard

Once it is established, DON CIO or the Navy (N6) will enable an "IA Dashboard" to facilitate DON management assessment of the state of information assurance in the Department. DON CIO and N6 will use the metrics listed in Appendix A to assist in updating the dashboard.

7. ANALYSIS OF GOALS

Each of the following goals is examined in three parts: assessment, objectives, and explanation.

Awareness and Training

The personnel who hold technical, operational, and procedural knowledge about information security are the most important resource of the DON information assurance efforts. The DON seeks to accomplish internal training programs that nurture information security expertise.

1. Assessment

The DON requires annual training in IA awareness and accepted information security practices of all employees who are involved with the management, use, or operation of DON systems. This includes on-site contractors as well as DON employees. In addition, privileged users (e.g., system administrators) and DAAs require specific training.

2. Objectives

- Conduct annual training of all DON personnel on information security concepts.
- Accomplish training and certification for all personnel engaged in administering information systems, including Designated Approving Authorities.

3. Actions

- DON organizations shall provide all personnel with annual information security awareness training, and maintain records of completion.
- DON organizations shall ensure compliance with specific training, certification, and reporting requirements for system administrators and DAAs, as defined in DoDD 8570.1 and its associated manual, DoD 8570.1M.

Capital Planning

The purpose of this goal is to ensure that information security plays a prominent role in the acquisition planning cycle and to ensure that newly acquired products meet DoD guidance.

1. Assessment

As OMB pointed out in its FY 2001 report, the rapid pace of product development makes it essential that government organizations assess the risks associated with using new commercial technology. Since 1 July 2002, DON is required to acquire commercial-off-the-shelf (COTS) IA and IA-enabled products that meet the criteria established by NSTISSP-11, as discussed in paragraph E3.2.5 of DoDI 8500.2 (Information Assurance Implementation).

2. Objectives

- Ensure that information security plays an integral role in acquisition and information technology investment planning.
- Procure and deploy the best information security solutions available from the marketplace and maintain the support infrastructure needed to deliver technical assistance to operational users.
- Ensure that all security products meet the common criteria profiles established by NIAP.

3. Action

- DON components shall acquire and use evaluated or validated Government-off-the-shelf (GOTS) or COTS IA and IA-enabled IT products for National Security Systems (NSS) in accordance with NSTISSP-11 and DoDI 8500.2.

Incident Response

The Navy and Marine Corps currently maintain standard incident response procedures that comprise the foundation of DON's incident response capability. DON CIO is working with the Navy and Marine Corps to facilitate seamless awareness of vulnerability actions and status to the DON leadership.

1. Assessment

Navy commands report incidents to the Navy Cyber Defense Operations Command (NCDOC) at Little Creek, VA. (NCDOC is also the Navy's CND Service Provider responsible to JTF-GNO). NCDOC has the specific mission to identify and respond to network security incidents. NCDOC reports the incidents to the Joint Task Force for Global Network Operations (JTF-GNO) via the Joint CERT Database (JCD) and the Joint Threat Database (JTD). Additionally, NCDOC coordinates Navy responses to the JTF-GNO-issued IAVAs. NCDOC monitors network traffic continually between Navy networks and the Defense Information Infrastructure (DII) for network intrusions, incidents, and anomalies and provides appropriate impact assessment and response in real time.

Marine Corps commands report incidents to the Marine Corps Network Operations and Security Command (MCNOSC) in Quantico, Virginia. The Marine Corps has established incident reporting procedures that detail reporting requirements from the end user to MCNOSC. This information is reported to the JTF-GNO via the JCD and the JTID. All reportable incidents are placed in the Marine Corps CERT Database (MCD), which in turn are released to the JCD. Marine Corps responses to IAVAs are also coordinated by MCNOSC via the Marine Corps Systems Command (MARCORSYSCOM) for Programs Of Record. MCNOSC (MARCERT) monitors network traffic continually between the Marine Corps Enterprise Network (MCEN) and the DII for network intrusions, incidents, and anomalies and provides appropriate impact assessment and response in near real time using IDSs, IPSs, Trend Analysis, and Correlation Tools.

Incident reporting data can provide multiple indicators regarding departmental compliance with policies and procedures and the effectiveness and efficiency of security service delivery. Thus, DON seeks to improve reporting mechanisms to keep DON leadership apprised of information assurance incidents.

2. Objectives.

- Maintain strong incident reporting and response capabilities by using current component operations.
- Improve DON senior management insight to DON incident response operations.
- Establish formal reporting mechanisms to provide DON with accurate incident reporting statistics anytime.
- Ensure that DON components use incident reporting data to assess their overall information security posture and provide that analysis to DON monthly.
- Review and update policies and procedures based on incident analysis.
- Use incident reporting data to predict future resource demands and allocate resources most effectively.

3. Actions

- DON components shall maintain formal reporting mechanisms to ensure prompt incident reporting.
- DON CIO will obtain unclassified data on information security incidents from NIOC and MCNOSC web sites at least weekly.
- The Department will use incident reporting data and analysis to evaluate the overall state of the DON information security program and identify possible policy or procedural improvements.

Risk Analysis and Management Oversight

Risk assessment is the process of analyzing threats to an IT system, and the potential impact that the loss of information or capabilities of a system would have on DON's mission. Program managers use the resulting analysis as a basis for identifying appropriate and effective actions to

mitigate risk. DoD, as discussed in the POA&M policy in Appendix B, states that full accreditation may be awarded although a system may contain Category-3 and Category-2 mitigated security deficiencies. Every effort should be taken to mitigate outstanding security deficiencies by building defense-in-depth mechanisms surrounding those systems.

The central method for analyzing and managing risks is the certification and accreditation process conducted in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (or its successor DIACAP) or Director Central Intelligence Directive (DCID) 6/3, as appropriate. In addition, the DISA Connection Approval Process (CAP) databases are used for monitoring network circuits.

- DITSCAP (or its successor DIACAP) is the process chiefly concerned with certifying and accrediting those systems and applications that are unclassified or classified through the Secret level. C&A progress is tracked within the DITPR-DON.
- DCID 6/3 is the C&A process for those systems classified as Top Secret/ SCI for the all of DoD. The process is monitored through the Office of Naval Intelligence (ONI) for DON systems.
- The DISA Connection Approval Process certifies and authorizes networks for connection. The process supports the C&A requirements of the network foundation infrastructure, to include monitoring centers within each Regional Network Operations and Security Center (RNOSC), the Network Information Center (NIC), and user enclave accreditation requirements.

FISMA requires annual self-assessments of information security. DoDI 8500.2 and NIST Special Publication 800-53 (*Recommended Security Controls for Federal Information Systems*) provide criteria for determining the current status of information security programs, enabling the establishment of targets for improvement. The DON should strive to test the effectiveness of policies and procedures by conducting annual assessments of information security, initiating reviews by the Naval Audit Service, and using the various NSA-chartered teams (e.g., Red, Blue, Green, and White Teams). Because of the major role the Navy Marine Corps Intranet (NMCI) plays in information security, oversight of the Service Level Agreements (SLAs) for IA in NMCI is particularly important.

1. Assessment

System C&A compliance is monitored through the DITPR-DON resident within DADMS. It is incumbent on the program managers and commanders of DON organizations to keep DITPR-DON accurate and up-to-date. OSD and DON CIO DITPR Guidance requires updates at least quarterly, and as changes occur. The DITPR-DON is uploaded to the DoD's DITPR at least quarterly or as required. OSD uses its DITPR to prepare the annual FISMA Report and to make quarterly progress reports to OMB. For networks, DISA maintains NIPRNET and SIPRNET CAP databases. OSD uses these databases for the network status input for FISMA reports.

In keeping with the specific FISMA requirement to conduct an annual assessment of information security programs, DON coordinates with the Naval Audit Service to conduct IA audits on various aspects of FISMA compliancy. Over and above this coordination, DITSCAP (or its

successor DIACAP) requires annual assessments of information systems, while the Navy and Marine Corps also assesses information security in accordance with FISMA.

While many of the NMCI services emphasize end-to-end performance within an agreement from a user perspective, a number of enterprise-level security services are viewed as mission critical and should be measured. Director NMCI monitors performance of the NMCI SLAs for the range of information security functionality provided with NMCI.

2. Objectives

- Establish reporting standards for DON C&A requirements.
- Integrate the C&A process with aspects of acquisition management.
- Update the DITPR-DON as changes occur and at least quarterly.
- Maintain current network status in the CAP NIPRNET and SIPRNET databases.
- Establish with the Naval Audit Service a schedule of independent evaluations of DON information security programs and practices.
- Conduct internal assessments of information security.
- Use the assets of Blue, Green, and White Teams to assist risk management.
- Establish regular Red Team exercises that test DON's information security architecture.

3. Actions

- DON organizations shall use the DITPR-DON and CAP databases, along with their update processes, to examine those systems, applications, or networks that are either unaccredited or operating under an interim authority to operate (IATO) or an interim authority to connect (IATC), respectively.
- DON CIO will cement the authoritative relationship between DON CIO and the Naval Audit Service by meeting with Naval Audit Service's points of contact early in the fiscal year to discuss the upcoming year's efforts. Establish agreements regarding:
 - Naval Audit Service's role in the DON information assurance efforts.
 - Expected Naval Audit Service contributions to annual DON FISMA report.
 - Coordination and reporting procedures.
 - Areas and organizations to be assessed or audited.
 - Reporting dates and subject of reports conducted per year.
- Navy and Marine Corps conduct annual assessment of information security in accordance with FISMA and DITSCAP (or its successor DIACAP) requirements.
- Program Managers use the concept of defense-in-depth as much as possible to mitigate outstanding security risks in systems and networks.

8. CONCLUSION

Through the cooperation of DON component organizations, DON CIO will improve information assurance, and thereby comply with FISMA. As mentioned previously, this improvement may be achieved by:

- Acknowledging the shortfalls identified in previous OMB, DoD, audit organizations, and DON reviews.
- Establishing goals that advance the DON information assurance program.
- Instituting well-defined sets of performance metrics.
- Conducting audits and assessments of information security.
- Maintaining a tiered approach to training- and awareness-based level of responsibility.
- Re-enforcing and rewarding good behavior and security practices, and modifying substandard behaviors and security practices, to include conducting additional training as may be required.

The goals and methodology of this plan are designed not only to identify and correct potential weaknesses in the DON information security posture, but also to provide an adequate framework for progress and evaluation. The DON CIO and staff stand ready to assist with the technical and policy challenges presented by the requirements of FISMA. It is important to note that that all DON personnel, including commanders, functional area managers, program managers, and all DON IT users (including military, civilian, and contractors) are expected to share the responsibility for IA and for FISMA compliance.

Metric	Description	Organization Reporting	Data Source	Frequency of Reporting	Reference	Goal	Required by OMB guidance for			
							FISMA 2005	FISMA 2004	FISMA 2003	GISRA 2002
OBJECTIVE 1: AWARENESS AND TRAINING										
1	Percentage of personnel (military, civilian, on-site contractors) who have received security awareness training	DCIO(N), DCIO(MC)		Annually	FISMA	100%	Y	Y	Y	Y
2	Percentage of personnel with specialized IT security responsibilities who have received security training (IA Officer [IAO], IA Manager [IAM])	DCIO(N), DCIO(MC)		Annually	FISMA	100%	Y	Y	Y	Y
3	Percentage of Designated Approving Authorities (DAA) who have received DAA training	DCIO(N), DCIO(MC)		Annually	FISMA	100%	Y	Y	Y	N
OBJECTIVE 2: CAPITAL PLANNING										
4	Percentage of Capital Asset Plans and Justifications (Exhibits 300) that are for fully accredited systems	ASN(FM&C)		Annually	FISMA	100%	Y	Y	Y	Y
5	Percentage of Exhibits 300 for non-accredited systems that have a POAM for completion	ASN(FM&C)		Annually	FISMA	100%	Y	Y	Y	N
OBJECTIVE 3: INCIDENT RESPONSE										
6	Percentage of IA Vulnerabilities Alerts (IAVA) closed on time	NIOC/MCNOSC		Quarterly	None	100%	N	N	N	N
7	Number of incidents (attempted penetrations), broken down into type and level of success	NIOC/MCNOSC	Websites	Weekly	None	NA	Y	Y	N	N
8	Percentage of attempted penetrations blocked	NIOC/MCNOSC		Annually	None	100%	Y	Y	Y	N
OBJECTIVE 4: RISK ANALYSIS AND MANAGEMENT OVERSIGHT										
9	Number of IA-related Material Weaknesses reported to ASN(FM&C)	DON CIO		Annually	FISMA	0%	Y	Y	Y	Y
10	Percentage of IA-related Material Weaknesses repeated in current FY	DON CIO		Annually	FISMA	0%	Y	Y	Y	Y
11	Percentage of systems in DON IT Registry with complete FISMA data	DON CIO, Components	DITPR-DON	Monthly	FISMA	100%	N	N	N	N
12	Percentage of systems with current final Authority to Operate (ATO)	DON CIO, Components	DITPR-DON	Monthly	FISMA	90%	Y	Y	Y	Y
13	Percentage of systems with either current ATO or Interim ATO (IATO)	DON CIO, Components	DITPR-DON	Monthly	FISMA	100%	Y	Y	Y	Y

METRICS MATRIX

Metric	Description	Organization Reporting	Data Source	Frequency of Reporting	Reference	Goal	Required by OMB guidance for			
							FISMA 2005	FISMA 2004	FISMA 2003	GISRA 2002
14	Percentage of systems with up-to-date Security Plan	DON CIO, Components	DITPR-DON	Monthly	FISMA	100%	Y	Y	Y	Y
15	Percentage of systems for which security controls have been tested and evaluated within the past 12 months	DON CIO, Components	DITPR-DON	Monthly	FISMA	100%	Y	Y	Y	Y
16	Percentage of systems for which Contingency Plan has been tested or evaluated within the past 12 months	DON CIO, Components	DITPR-DON	Monthly	FISMA	100%	Y	Y	Y	Y
17	Percentage of seats capable of cryptographic logon	DON CIO, Components		Quarterly	None	100%	N	N	N	N
18	Number of Red, Blue, Green, and White Team visits and assessments	Components		Annually	None	NA	Y	Y	N	N

Appendix B – FISMA Plan of Action and Milestones (POA&M) Process

1. A plan of action and milestones (POA&M) is a tool identifying tasks that need to be accomplished to remediate any identified vulnerabilities in a program or system. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

2. The purpose of a POA&M is to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The Office of Management and Budget (OMB) requires agencies to prepare POA&Ms for all programs and systems where an information technology (IT) security weakness has been found. OMB guidance directs chief information officers (CIOs) and program officials to develop, implement, and manage IT Security POA&Ms for all programs and systems they operate and control (e.g., this includes all systems that support their operations and assets, including those operated by contractors). Additionally, OMB requires program officials to regularly (at least quarterly) update the CIO on their progress, in order to enable the CIO to monitor Department of the Navy (DON)-wide remediation efforts and provide the required quarterly update to OSD for forwarding to OMB.

3. The IT Security POA&M is a living document designed to be a management tool to assist in closing their security performance gaps, assist inspectors general (IGs) in their evaluation work of security performance, and assist DON CIO, OSD, and OMB with oversight responsibilities. DON IT Security POA&Ms shall:

3.1. Be tied to the Department's budget submission when required through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.¹

3.2. Include all IT security weaknesses found during any other review done by, for, or on behalf of the Department, including but not limited to those found by audit agencies, financial system audits, official security test and evaluation or compliance review, and critical infrastructure vulnerability assessments.

3.3. Follow the format detailed in the examples provided by the OMB and shown below.

3.4. Be submitted to the respective DON Deputy CIO (Navy or Marine Corps).

3.5. Be submitted by the Deputy CIO to the DON Senior Information Assurance Officer (SIAO) if directed.

4. When there is compelling operational necessity, DON information systems may be allowed to operate despite IT security weaknesses that cannot be corrected or adequately mitigated within prescribed timeframes because of technology limitations or, in rare cases, prohibitive costs. Such instances must be fully justified, approved, and documented as described below.

¹ OMB Circular A-11 requires that agencies develop and submit to OMB business cases (Exhibit 300) for major IT projects. Additionally, each agency submits an Exhibit 53, a list of both major and non-major IT systems.

Appendix B – FISMA Plan of Action and Milestones (POA&M) Process

Types of IT Security POA&Ms and Severity Codes

4.1 There are three types of IT Security POA&Ms as reflected in Table 1 and further described in paragraphs below.

Table 1
Types of DON IT Security POA&Ms

Report	Responsibility	Submit To	Dates
System Level POA&Ms (Table 2)	Program Managers (PM)	DON Deputy CIO (Navy or Marine Corps) and; DON SIAO: All systems with a CAT I weakness or on OMB Watch List (Exhibit 300s) for security	1 Dec, 1 Mar, 1 Jun, 1 Sep
DON level Significant Deficiency POA&M (Table 3)	DON CIO	OSD (NII)	1 Dec, 1 Mar, 1 Jun, 1 Sep
DoD Enterprise POA&M	OSD (NII)	OMB	As directed

4.2. Severity Codes are assigned to a system weakness by a Certification Authority (CA) or his designated representative as part of a certification analysis to indicate (1) the risk level associated with the security weakness and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as “CAT-I, CAT-II, or CAT-III,” where CAT-I is the indicator of greatest risk and urgency. CAT-I weaknesses shall receive the highest priority for correction or mitigation. Severity codes are assigned after consideration of all possible mitigation measures have been taken within system design/architecture limitations for the information system in question. For instance, what may be a CAT-I weakness in a component part of a system (e.g., a workstation or server) may be offset or mitigated by other protections within hosting enclaves such that the overall risk to the system is reduced to a CAT-II.

4.2.1. CAT-I weaknesses allow primary security protections or perimeters to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges (e.g., root privileges), and cannot be satisfactorily mitigated. CAT-I weaknesses shall be corrected before an Authorization to Operate (ATO) is granted. A system can operate with a CAT-I weakness only when the system is critical to military operations and failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. Only the respective DON Deputy CIO (Navy or Marine Corps) shall authorize operation of a system with a CAT-I weakness and this can only be done through an Interim Authorization to Operate (IATO). This responsibility cannot be delegated below the DON

Appendix B – FISMA Plan of Action and Milestones (POA&M) Process

Deputy CIO. The DON Deputy CIO shall provide a signed copy of the authorization memorandum with supporting rationale to the DON SIAO for forwarding to the DoD SIAO.

4.2.2. CAT-II weaknesses are those that can lead to unauthorized system access or activity but can usually be corrected or mitigated to a point where any residual risk is acceptable. CAT-II weaknesses must be corrected or satisfactorily mitigated before an ATO can be granted. If CAT-II weaknesses cannot be corrected or satisfactorily mitigated within the time limitation imposed in the IATO, the DAA must certify in writing that continued system operation is critical to mission accomplishment or terminate system operation. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DON Deputy CIO.

4.2.3. CAT-III weaknesses, if corrected, will improve the system's IA posture but do not preclude an authorization to operate. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT-III weaknesses accepted by the DAA will show scheduled completion date as N/A, note acceptance by DAA in the milestone column, and risk accepted in the status column.

4.3. A POA&M shall be prepared for DON information systems with a current ATO that are found to be operating in an unacceptable IA posture through audits or other reviews or events, such as an annual security review or compliance validation. An unacceptable IA posture results when the IA Controls compliance posture does not match that authorized by the Accreditation Decision. For example an IA Control is found to be non-compliant or a satisfactory mitigation is not in place, leading to a newly identified weakness. If the information system already has an IT Security POA&M, the newly identified weakness will be added.

4.3.1. If a newly discovered CAT-I weakness on a DON information system operating with an ATO cannot be corrected within 30 days, the system can continue operation only under the terms prescribed in paragraph 4.2.1. above.

4.3.2. If a newly discovered CAT-II weakness on a DON information system operating with a current ATO cannot be corrected or satisfactorily mitigated within 90 days, the system can continue operation only under the terms prescribed in paragraph 4.2.2. above.

5. DON Deputy CIOs are responsible for monitoring and tracking the overall execution of system level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The PMs or IA Managers are responsible for implementing the corrective actions identified in IT Security POA&Ms and providing visibility and status to the DAA and the governing DON Deputy CIO.

5.1. IT Security POA&Ms are permanent records. Weaknesses posted become part of that record and will be updated, but not removed after correction or mitigation actions are completed. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

5.2. Table 2 below is an example of a completed system level IT Security POA&M, illustrating the appropriate level of detail required. Included in the heading of the system level

Appendix B – FISMA Plan of Action and Milestones (POA&M) Process

IT Security POA&M template is a field for OMB Project Identification (ID) and Security Costs which must be filled in from Exhibits 300 and 53, where applicable.

5.3. Once an initial system level IT Security POA&M weakness has been opened, no changes may be made to the data in columns 1 (Weakness), 6 (Scheduled Completion Data), 7 (Milestones with Completion Dates), and 9 (Identified in Chief Financial Officer (CFO) Audit or other Review).

5.4. IT Security POA&Ms listing CAT-I or CAT-II weaknesses shall be assessed for classification. For instance, the fact that a Mission Assurance Category (MAC) I or II information system has a CAT-I weakness that has not been mitigated to a degree that will preclude immediate unauthorized access dictates a minimum classification of CONFIDENTIAL. Other factors that would influence a classification decision include the number of CAT-II weaknesses identified for a single system and whether the system itself is classified.

5.5. The following instructions explain how a system level IT Security POA&M should be completed.

Column 1 – Type of security weakness. Describe security weaknesses identified during certification or by the annual program review, audit, or any other work done by or on behalf of the program office or Service. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the IT Security POA&M should note the fact of its special sensitivity and should be classified accordingly. Where more than one weakness has been identified, number each individual security weakness as shown in the examples.

Column 2 – CAT (Severity Code). Code assigned to a system deficiency by a CA as part of certification analysis to indicate (1) the risk level associated with the deficiency and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as “CAT-I, CAT-II, CAT-III” where CAT-I is the indicator of greatest risk and urgency. POA&Ms with CAT-I weaknesses will normally be classified.

Column 3 – Security Control. An IA Security Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Security Control are assignable and thus accountable. IA Security Controls are assigned according to MAC (for Integrity and Availability) and Confidentiality Level in accordance with DoDI 8500.2.

Column 4 – POC. Identity of the office or organization that is responsible for resolving the security weakness.

Column 5 – Resources Required. Estimated funding or manpower (i.e., full time equivalents (FTE)) resources required to resolve the security weakness. Include the anticipated source of funding (i.e., within the system or as a part of a cross-cutting security infrastructure program). Include whether a reallocation of base resources or a request for new funding is anticipated. This

Appendix B – FISMA Plan of Action and Milestones (POA&M) Process

column should also identify other, non-funding, obstacles and challenges to resolving the security weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system).

Column 6 – Scheduled Completion Date. Scheduled completion date for resolving the security weakness. Please note that the initial date entered should not be changed. If a security weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in Column 10, “Status.” If risk is accepted for a CAT-II or CAT-III weakness, enter N/A.

Column 7 - Milestones with Completion Dates. A milestone will identify specific requirements to correct an identified weakness. Mitigation plan (actions) will be listed as a milestone in column 7. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones the agency should note them in the Column 8, “Milestone Changes.”

Column 8 - Milestone Changes. This column would include new completion dates for the particular milestone.

Column 9 – Source Identifying Weakness. Identify the source (e.g., program review, IG audit, GAO audit, DoDI 8500.2 controls review, etc.) that discovered the security weakness.

Column 10 – Status. Use one of the following terms to report status of corrective actions: Ongoing , Completed, or Risk Accepted for a CAT-II or CAT-III weakness that has been accepted by the DAA. “Completed” should be used only when a security weakness has been fully resolved and the corrective action has been tested. Include the date of completion or risk accepted for a weakness.

Column 11 – Comments. Include any amplifying or explanatory remarks that will assist in understanding other entries relative to the weakness.

Date Initiated:	October 1, 2006			POC Name:	John Smith		OMB Project ID:*			
Date Last Updated:	January 10, 2007			POC Phone:	703-555-5555		009-222334-55874			
Component Name:	DON			POC E-mail:	w.t.door@navy.mil		Security Costs: \$62500			
System/Project Name:	DON Network									
DoD IT Registration No.:										
Weakness	CAT	Security Control	POC	Resources Required	Complete By	Milestones with Completion Dates	Milestone Changes	Source Identifying Weakness	Status	Comments
An account management process has not been implemented to ensure that only authorized users can gain access to the DoD network and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	I**	IAAC-1 Impact High	IAO	\$50,000	5/30/2005	Develop an account Management Process - 1/15/2005; Management Review of account management process 3/15/2005; Implement/Test account management process 4/15/2005	Implementing and Testing the account management process delayed till 10/15/2005 due to inadequate funding.	8500.2 Controls Test Conducted 5/15/2005	Ongoing	Funding will be available in FY 2006
Security plan is out of date, more than one year since last update despite new interconnections	II	DCSD-1 Impact High	IAO	\$5,000	11/30/2005	Update plan and obtain independent review 11/30/2005		8500.2 Controls Test Conducted 5/15/2005	Ongoing	
Lack of accurate system hardware and software baseline hampers implementation of Configuration Management processes.	II	DCHW-1/DCSW-1 Impact High	IAO	\$0	8/31/2005	Establish baseline inventory of the hardware and software and utilize revision control system -6/15/2005. Implement a software revision control program. - 8/31/2005.		Security Test and Evaluation - 4/15/2005	Completed 10/30/2005	
Encryption is not certified FIPS 140-2 compliant.	III	DCNR-1 Impact Medium	IAO	\$5,000	10/21/2005	Upgrade encryption software to FIPS 140-2 certified version 10/21/2005		IG Audit 3/21/2005	Ongoing	May slip due to delay in funding
Audit application does not record certain actions.	II	ECAR-2 Impact Medium	IAO	\$2,500	9/30/2005	(1) Prohibit simultaneous log- on of SAs and ISSOs, (2) Ensure physical logs are maintained, 6/15/2005(3) Provide instructions for configuring additional required audits, 7/15/2005and (4) Require periodic review of the local authorized users list to ensure its accuracy and currency.9/15/2005		8500.2 Controls Test Conducted 5/15/2006	Completed	

Table 2
System Level POA&M

*Cite unique project ID and name shown on Exhibit 300 and security costs from Exhibit 53, if applicable

** Classify as appropriate. Actual CAT-I is minimally CONFIDENTIAL.

APPENDIX B – FISMA Plan of Action and Milestones (POA&M) Process

6. DON CIO required to complete and submit a DON-level significant deficiency IT Security POA&M as indicated in Table 1.

6.1. A DON-level IT Security POA&M is required for the following:

6.1.1. Systemic weaknesses (significant deficiencies) identified across the Department.

6.1.2. Systemic weaknesses (significant deficiencies) identified by audits and reviews.

6.2. Table 3 below contains an example of a completed DON-level IT Security POA&M, illustrating the appropriate level of detail required. Once DON CIO has completed the initial DON-level IT Security POA&M, no changes should be made to the data in columns 1 (Weakness), 4 (Scheduled Completion Date), 5 (Milestones with Completion Dates), and 7 (Source Identifying Weakness).

6.3. The DON-level IT Security POA&M should be filled out using the instructions above for a system level IT Security POA&M, however, the Security Control column does not apply for a DON-level IT Security POA&M.

7. The DoD CIO is responsible for completing a DoD Enterprise IT Security POA&M that will be provided as indicated in Table 1 above, using OSD's own format. This POA&M identifies DoD significant deficiencies that are systemic across the Department. The DoD CIO reports on Systemic deficiencies in the Enterprise IT Security POA&M, derived from the DoD Component-level quarterly significant deficiency IT Security POA&Ms, GAO and IG audits, and other reviews and events.

Date:	March 1, 2005	POC Name:	Mr. Navy CIO				
Component Name:	DON	POC Phone:	555-555-1234				
		POC E-mail:	doncio@nav.mil				
Weakness	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Milestone Changes	Identified in CFO Audit or other Review	Status
Annual testing of contingency plans not being conducted	Component CIO	700K	3/1/2006	Verify and test contingency plans for 98% of systems C&A 12/30/05		Annual review	Ongoing
Security Awareness, Training, and Education - no process for tracking completion of specialized training	Component CIO	200K	10/1/2005	Implement and test training database 6/1/05 Enter personnel requiring specialized training into database 10/1/05		OIG Audit	Ongoing
Inconsistent and inadequate personal computer inventory afloat	Component CIO	500K	10/1/2006	Implement and test afloat computer inventory system 10/1/05 Enter 50% afloat inventory into database 3/1/06 Enter 100% afloat inventory into database 10/1/06		Naval Audit Service	Ongoing

Table 3
DON-Level Significant Deficiency POA&M

APPENDIX C

Acronyms

Definitions are found in DoDD 8500.1, DoDI 8500.2, and CNSS Instruction 4009 of May 2003.

ASN	Assistant Secretary of the Navy
C&A	Certification and Accreditation
CAP	Connection Approval Process
CERT	Computer Security Emergency Response Team
CIO	Chief Information Officer
CJCSM	Commander Joint Chief of Staff Manual
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CNSS	Committee on National Security Systems (formerly the Committee on National Security Telecommunications and Information Systems Security)
COTS	Commercial-Off-the-shelf
DAA	Designated Approving Authority
DADMS	DON Application and Database Management System
DCID	Director Central Intelligence Directive
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DIACAP	DoD Information Assurance Controls Verification and Authorization Process
DITPR	DoD Information Technology Portfolio Repository
DITPR-DON	DITPR (Department of the Navy)
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoD-IG	DoD Inspector General
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
FISMA	Federal Information Security Management Act
FM&C	Financial Management and Comptroller
GOTS	Government-off-the-shelf
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer

IATC	Interim Approval to Connect
IATO	Interim Approval to Operate
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IA	Information Assurance
IT	Information Technology
JCD	Joint CERT Database
JTID	Joint Threat Intelligence Database
JTF-GNO	Joint Task Force-Global Network Operations
MAIS	Major Automated Information System
MARCERT	Marine Corps Computer Security Emergency Response Team
MCD	Marine Corps CERT Database
MCNOSC	Marine Corps Network Operations and Security Command
MDAP	Major Defense Acquisition Program
MILDEP	Military Department
NCDOC	Navy Cyber Defense Operations Command
NCTF-CND	Navy Component Task Force-Computer Network Defense
NIAP	National Information Assurance Partnership
NIC	Network Information Center
NIOC	Navy Information Operations Command
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Science and Technology
NMCI	Navy Marine Corps Intranet
NSA	National Security Agency
NSS	National Security Systems
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence
OSD	Office of the Secretary of Defense
POA&M	Plan of Actions and Milestones
RNOSC	Regional Network Operations and Security Center
SCI	Sensitive Compartmented Information
SECNAVINST	Secretary of the Navy Instruction
SIPRNET	Secret Internet Protocol Router Network
SLA	Service Level Agreement