



DEPARTMENT OF DEFENSE  
6000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-6000

MAY 02 2008

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
COMMANDERS OF THE COMBATANT COMMANDS  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION  
DIRECTOR, NET ASSESSMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Federal Information Security  
Management Act (FISMA) Guidance - Fiscal Year 2008 (FY08)

FISMA requires that agency heads and inspectors general evaluate their agency's information security programs and report the results of those evaluations to the Office of Management and Budget (OMB), Congress, and Government Accountability Office (GAO) in October of each year. This memorandum establishes procedures and reporting guidelines for the CIO information security portion of the FY08 DoD report. The DoD Privacy Official will issue separate guidance on the privacy section of the report.

To help assure accurate and consistent reporting across the Department, the following attachments are provided:

- Attachment 1: System registration information and points of contact;
- Attachment 2: Instructions for completing the OMB/DoD templates;
- Attachment 3: Details for entering FISMA-related data into the DoD IT Portfolio Repository (DITPR) and SIPRNET IT Registry;
- Attachment 4: Annual security review and security controls testing;
- Attachment 5: IT Contingency Plan (CP) development and testing;
- Attachment 6: Information Assurance (IA) workforce data collection;



- Attachment 7: Security Plan of Action and Milestones (POA&M);
- Attachment 8: Relevant definitions;
- Attachment 9: OMB templates (Microsoft Excel®) with DoD-specific spreadsheet additions. This is the file you will use to submit your responses.

The Department's goal is a 100% compliance with certification and accreditation (C&A), annual security reviews, contingency plans tested, security controls tested, and training requirements. The submission of the annual FISMA Report is due to this office by July 18, 2008.

Please continue to make this effort a priority. Questions regarding this matter may be directed to Mr. John Hunter, (703) 602-9927, (DSN) 332-9927, john.hunter@osd.mil or john.hunter@osd.smil.mil, or Mr. Charles Schaffer, (703) 604-1489 ext.168, (DSN) 664-1489, charles.schaffer.ctr@osd.mil or charles.schaffer.ctr@osd.smil.mil.

  
John G. Grimes

Attachments:  
As stated

ATTACHMENT 1

SYSTEM REGISTRATION AND POINT OF CONTACT LIST

1. INTRODUCTION. The DoD FISMA report will address Information Assurance (IA) throughout the Department. This attachment provides overarching guidance for completing the Chief Information Officer (CIO) Section of the Office of Management and Budget (OMB) and DoD templates (Attachment 9) and identifies those responsible for completing each subsection. The following key points need to be considered when completing Component inputs to the DoD FISMA report.

a. All data should be entered and saved in these templates and returned upon completion **no later than July 18, 2008**. They should have a cover letter, signed by the Component CIO, attesting to the accuracy of the information. Attachment 2 of this guidance provides specific instructions for completing the templates.

b. Please ensure that if any portion of the report is classified that it is submitted through the Secret Internet Protocol Router Network (SIPRNET).

c. DoD Components will be permitted to provide an updated status of system and training metrics until August 29, 2008. DoD Component reports will be incorporated into the Department's final report submitted to OMB and Congress in September 2008.

d. It is possible that OMB will issue additional guidance later this year. If necessary, DoD will promulgate supplemental guidance.

e. DoD IT Portfolio Repository (DITPR) and SIPRNET IT Registry Information:

(1) These are the databases of record for FISMA reporting. Guidance for completing the FISMA-related fields in the databases is provided in Attachment 3.

(2) As a reminder, for reporting consistency the information security data in the Select and Native Programming – IT (SNaP-IT) database for Capital Investment Reports (Exhibit 300s) must match the information security information in these databases.

(3) The Office of the Secretary of Defense (OSD) uses these databases to compile the system metrics (Q.1. and Q.2.) of the FISMA report. The DITPR is located on the Non-secure Internet Protocol Router Network (NIPRNET) at <https://ditpr.dod.mil/> and the SIPRNET IT Registry is at <https://147.254.164.141>.

(4) Components shall enter and maintain FISMA data for each entry that requires a C&A, and update and maintain their Component's input at least quarterly. However, Components are encouraged to update their data as changes occur. Quarterly updates must be completed no later than February 13, 2008, May 14, 2008, August 13, 2008, and November 12, 2008. The annual update must be completed no later than August 27, 2008.

(5) Intelligence System Reporting:

(a) All DoD Intelligence systems not handling sensitive compartmented information (SCI) or special access program (SAP) information must be entered in either the DITPR on the NIPRNET or the SIPRNET IT Registry.

(b) DoD Intelligence Systems handling SCI or SAP information, however, should be registered in accordance with guidance provided by the Director of National Intelligence (DNI) Office of the Chief Information Officer (CIO).

(6) Entry of FISMA information for IT systems. The classification of the information about the IT system is determined by the Component. The classification level should be used to determine which DoD inventory system to use for FISMA reporting.

(a) All DoD systems having unclassified information describing the system must be entered in the DITPR on the NIPRNET.

(b) DoD systems having Confidential or Secret information describing the system must be entered in the SIPRNET IT Registry.

(7) IAW Deputy Chief Information Officer Memorandum, December 21, 2004, "Department of Defense (DoD) Information Technology (IT) Registry Guidance for Fiscal Year 2005 (FY05)", 100% of all systems should have been entered into the DITPR/SIPRNET IT Registry by September 30, 2006.

f. Significant parts of the FISMA report are metrics related to the DoD Information Assurance Certification and Accreditation Process (DIACAP). To help assure accurate and consistent reporting from Components, several attachments are included in this guidance. Attachment 4 covers the annual security review and IA controls testing. Attachment 5 is devoted to IT Contingency Plan (CP) development and testing guidance. Attachment 6 provides instructions for IA workforce and training data collection while Attachment 7 provides a brief coverage of IT security Plan of Action and Milestones (POA&M). Relevant definitions are provided in Attachment 8.

2. POINT OF CONTACT (POC) LIST

a. DIAP FISMA

Mr. John Hunter	(703) 602-9927	john.hunter@osd.mil
Mr. Charles Schaffer	(703) 604-1489 ext. 168	charles.schaffer.ctr@osd.mil
Mr. Freddie Beaver	(703) 604-1489 ext. 173	freddie.beaver.ctr@osd.mil
Ms. Virginia Ephraim	(703) 604-1489 ext. 165	virginia.ephraim.ctr@osd.mil

b. DIAP FISMA Compliance

Mr. David Hollis	(703) 602-9982	david.hollis@osd.mil
Mr. Shawn Simmons	(703) 604-1489 ext. 111	shawn.simmons.ctr@osd.mil

c. DoD IA Training

Mr. Steven Busch	(703) 604-1489 ext. 112	steve.busch.ctr@osd.mil
Mr. Ben Scribner	(703) 604-1489 ext. 137	benjamin.scribner.ctr@osd.mil

d. IC CIO

Mr. Thanh Nguyen	(703) 874-8845	thanhn@dni.gov
------------------	----------------	----------------

e. DITPR Helpdesk

Helpdesk Support	(703) 506-5220	DITPR@att.com
------------------	----------------	---------------

f. SIPRNET IT Registry Helpdesk

Mr. David Griffin	(703) 602-2525 ext. 224	david.griffin.ctr@osd.mil
Ms. Mogana Richards	(703) 602-2525 ext. 221	mogana.richards.ctr@osd.mil

g. DITPR and SIPRNET IT Registry

Mr. Leslie Bloom	(703) 601-4729 ext. 110	leslie.bloom@osd.mil
Mr. Kevin Garrison	(703) 347-4920	kevin.garrison.ctr@osd.mil

ATTACHMENT 2

OMB AND DOD REPORTING TEMPLATES INSTRUCTIONS

1. SECTION B OMB TEMPLATE, QUESTIONS 1 AND 2. The following explains the included templates (Attachment 9) that require completion as the primary response to the CIO portion (OMB Template, Section B) of the annual reporting requirement. This attachment provides specific information about what to enter into each required field. Section B, questions 1 and 2, are to be completed by DoD Components.

a. Question 1.a, (**Agency Systems**), and provide the total number of operational systems in the DITPR or SIPRNET IT Registry reported as Government (DoD) Owned and Government Operated (GOGO) or Government (DoD) Owned and Contractor Operated (GOCO). (Figure 1)

(1) Provide number of systems in designated rows by Mission Assurance Category (MAC) equivalents to Federal Information Processing Standards (FIPS) Publication 199 system impact level: MAC I (High), MAC II (Moderate), MAC III (Low), and any systems not categorized by MAC level.

(2) Note: Although the Confidentiality Level (CL) is an essential part of system categorization and control selection, it is not used here in order to provide a comparable listing to FIPS 199 levels reported by all other Federal agencies.

b. Question 1.b, (**Contractor Systems**), provide the total number of operational systems in the DITPR or SIPRNET IT Registry that are reported as Contractor Owned and Contractor Operated (COCO) on behalf of the DoD and Contractor Owned and Government (DoD) Operated (COGO). Provide number of systems in designated rows by MAC levels, the same as was done for question 1.a.

(1) Per Title III (FISMA) of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899) [<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>], COCO information systems are defined as those operated by a DoD contractor or another entity “on behalf of the DoD.”

(2) Reportable unclassified COCO systems are those that must be certified and accredited under the DIACAP. They include contractor systems that are dedicated to processing DoD information and are effectively under DoD configuration control (e.g., the Navy Marine Corps Intranet) and those that provide a direct service to a DoD customer (e.g., the Transportation Payment System).

(3) Contractor systems that process some DoD information ( e.g., that provided with requests for proposals or information developed by contractors during the execution of DoD contracts) but are not under DoD control or do not provide a direct service to the Department should not be listed in the DITPR or reported as COCO.

(4) All classified COCO systems are by their nature operated on behalf of the DoD and must be reported in the SIPRNET IT Registry, (with the exception of Intelligence Community (IC) contractor systems, which have a separate FISMA reporting structure.)

c. Question 1.c, automatic totaling, *no entry required*.

d. Question 1.d, paste the following required statement:

***“System impact levels determined using Mission Assurance Category (MAC) designations in accordance with DoD Directive 8500.01E, Information Assurance (IA).”*** In addition, if you have any systems listed as “Not Categorized” in questions 1.a or 1.b, provide a brief explanation here. (Figure 2)

e. Question 2.a, report the total number of both Authority to Operate (ATOs) and Interim Authority to Operate (IATOs) by MAC levels.

f. Question 2.b, the number of systems for which security controls have been tested and reviewed in the last year (see Attachment 4).

g. Question 2.c, identify the number of systems for which contingency plans have been tested in accordance with policy and guidance. This corresponds to the DITPR field “IT Contingency plan test” in accordance with guidance in Attachment 4.

Section B - Chief Information Officer: Questions 1 and 2											
Component: { component name }				Submis: Submission date: 07/18/08							
Question 1: FISMA Systems Inventory											
<p>1. In the table below, identify the number of agency and contractor information systems by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.</p> <p>Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.</p> <p>Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.</p>											
Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing											
<p>2. For the Total Number of Systems identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested within in accordance with policy.</p>											
		Question 1			Question 2						
		a. Agency Systems	b. Contractor Systems	c. Total Number of Systems (Agency and Contractor systems)	a. Number of systems certified and accredited			b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Component Name	FIPS 199 System Impact Level	Number	Number	Total Number	Total ATO	Total IATO	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
{ component name }	High			0							
	Moderate			0							
	Low			0							
	Not Categorized			0							
	Total		0	0	0	0	0	0	0	0	0
Note: Shaded cells are locked and auto-populated by data from related cells which permit entries from the Component.											

**Figure 1. OMB Template, Section B, Questions 1 and 2**

h. Question 2.d, provide explanation if any ATO totals (question 1.c) are higher than their tested CP totals (question 2.c), i.e. 1.c>2.c. Rationale: no system should have a valid ATO if the CP testing has never been done or is expired. (Figure 2)

i. Question 2.e, list ALL systems that are not accredited, (i.e. operational systems that have neither an ATO nor IATO.) Of these systems, provide the Unique Project Identifier (UPI) associated with the ones presented in your FY2009 Exhibit 53. Contact the appropriate Component POC for the list of Exhibit 53 systems.

Section B - Chief Information Officer: Questions 1 and 2 (continued)				
<b>Component: { component name }</b>				
<b>1.d.</b>	If there are systems which have not yet been categorized by system impact level, or, if a system impact level was determined through another method, please explain. Response:			
<b>2.d.</b>	If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain: Response:			
<b>2.e.</b>	For all systems reported as not having a C&A (Question 2.a. percentage is less than 100%), please identify the system by Component/Bureau, the system impact level, and the Unique Project Identifier (UPI) associated with the system as presented in your FY2009 Exhibit 53. Extend the table as necessary to include all systems without a C&A.			
<b>No.</b>	<b>Component/Bureau</b>	<b>System Name</b>	<b>System Impact Level</b>	<b>Exhibit 53 Unique Project Identifier (UPI)</b>
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
<b>Total Number of Systems without a C&amp;A:</b>		12		
* total auto-filled by number of rows in table above ("No." column count.) Insert as many rows as needed to account for all non-ATO operational systems; delete any extra rows.				

**Figure 2. OMB Template, Section B, Questions 1 and 2 (continued)**

*Note: These tables are template images of the Excel spreadsheets provided separately with this guidance and data should not be entered here. Provide all data reporting to DoD in the Excel spreadsheets (Attachment 9).*

2. SECTION B OMB TEMPLATE, QUESTIONS 3, 4, AND 5

- a. Questions 3.a. and 3.b. will be completed by OSD.
- b. Question 4.a. completed by all Components and consolidated by OSD.
- c. Question 4.b. will be completed by OSD.
- d. Question 5, (**Incidents**), to be completed by USSTRATCOM based on information provided by Joint Task Force-Global Network Operations (JTF-GNO) IAW their Unified Command Plan Computer Network Defense Mission.

<b>Section B - Chief Information Officer: Questions 3, 4, and 5</b>					
<b>Agency Name:</b>					
<b>Question 3: Implementation of Security Controls in NIST Special Publication 800-53</b>					
<b>3a.</b>	<p>Has the organization developed policies and corresponding procedures to cover all NIST SP 800-53 control families, and associated 800-53a controls? Yes or No.</p>				
<b>3.b.</b>	<p>Please describe your testing and continuous monitoring process: Response:</p>				
<b>Question 4: Incident Detection Capabilities</b>					
<b>4.a.</b>	<p>What tools, techniques, technologies, etc., does the agency use for incident detection? Response:</p>				
<b>4.b.</b>	<p>How many systems (or networks of systems) are protected using the tools, techniques and technologies described above?</p>				
<b>Question 5: Incidents</b>					
<p>Information gathered in this question will be supplemented by your agency's reporting to the United States Computer Emergency Readiness Team (US-CERT).</p> <p>Identify the number of successful incidents reported to US-CERT and the number of incidents reported to law enforcement. Explanatory comments can also be provided.</p>					
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; padding: 2px;">Incidents Reported to US-CERT</th> <th style="width: 50%; padding: 2px;">Incidents Reported to Law Enforcement</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"></td> <td></td> </tr> </tbody> </table>		Incidents Reported to US-CERT	Incidents Reported to Law Enforcement		
Incidents Reported to US-CERT	Incidents Reported to Law Enforcement				
<p>Explanatory Comments:</p>					

Figure 3. OMB Template, Section B, Questions 3, 4, and 5

3. SECTION B OMB TEMPLATE, QUESTIONS 6, 7, AND 8. These questions capture data on Security Awareness Training (Q6), Peer-to-Peer File Sharing (Q7) Awareness, and Configuration Management (Q8).

<b>Section B - Chief Information Officer: Questions 6, 7, and 8</b>							
<b>Agency Name:</b>							
<b>Question 6: Security Awareness Training</b>							
<b>6.a. Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Yes or No.</b>							
<b>6.b. Report the following for your agency:</b>							
<b>b.1.</b>	<b>b.2.</b>		<b>b.3.</b>	<b>b.4.</b>	<b>b.5.</b>		<b>b.6.</b>
Total number of employees	Number of employees that received IT security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003)		Number of employees that received IT security awareness training using an ISSLOB shared service (breakout of total for b)	Total number of employees with significant IT security responsibilities	Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)		Total costs for providing IT security training in the past fiscal year (in \$'s)
	Number	Percentage	Number		Number	Percentage	
		#DIV/0!				#DIV/0!	
<b>6.c. Briefly describe the training provided in 6.b.2 and 6.b.5:</b>							
Response:							
<b>Question 7: Peer-to-Peer file sharing</b>							
<b>Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.</b>							
<b>Question 8: Configuration Management</b>							
<b>8.a. Is there an agency wide security configuration policy? Yes or No.</b>							
<b>Approximate the extent to which applicable information systems apply common security configurations established by NIST.</b>							
<b>Response categories:</b>							
<b>8.b.</b>							
<ul style="list-style-type: none"> <li>- Rarely- for example, approximately 0-50% of the time</li> <li>- Sometimes- for example, approximately 51-70% of the time</li> <li>- Frequently- for example, approximately 71-80% of the time</li> <li>- Mostly- for example, approximately 81-95% of the time</li> <li>- Almost Always- for example, approximately 96-100% of the time</li> </ul>							

**Figure 4. OMB Template, Section B, Questions 6, 7, and 8**

a. Question 6: Security Awareness Training. Detailed instructions for IA Workforce data collection, which is aggregated to answer Q6, are provided in Attachment 6, *IA Workforce and Training Data Collection Instructions*.

(1) Question 6.a. (Ensured Security Awareness Training of all employees)  
This will be answered by OSD.

(2) Question 6.b.1. (Total number of employees in FY08) This value is automatically calculated from the value in the “Required” cell of Attachment 6, Table 3 (IA User Training).

(3) Question 6.b.2. (Number that received IT Security Awareness Training)  
This value is automatically calculated from the value in the “Completed” cell of Attachment 6, Table 3.

(4) Question 6.b.3. (Number of employees in question 6.b.2. that received training using an Information System Security Line of Business (ISS LoB) shared service) This value is automatically calculated from the value in the “DoD SSC” cell of Attachment 6, Table 3. Note: This is the number from the "Completed" total of Question 6.b.2 that received IA awareness training using the “DoD IA Awareness” training course developed by the DoD Shared Service Center (DoD SSC). See Attachment 6 for more information on the current policy for IA awareness training.

(5) Question 6.b.4. (Total number with Significant IT Security Responsibilities)  
This value is automatically calculated by adding the totals from the bottom row labeled “Total” of the columns “Civilian Filled”, “Military Filled”, and “Contractor Filled” from Table 1 (IA Workforce Primary Duty Positions) and Table 2 (IA Workforce Additional/Embedded Duty Positions) of Attachment 6.

(6) Question 6.b.5. (Number ...that received Specialized Training) This value is automatically calculated by adding the totals from the bottom row labeled “Total” of the columns “Civilian Trained”, “Military Trained”, and “Contractor Trained” from Tables 1 and 2.

(7) Question 6.b.6. (Total Costs for Providing IT Security Training in FY08)  
This number will automatically be carried over from Table 4 (IA Workforce Milestone Budget Plans (training and certification, costs), row “Obligated” column FY08.

(8) Question 6.c. (Training Description) Provide the details of the Awareness and Specialized training in FY08. If you wish, you can also include metrics and lessons learned in the “Response” block.

b. Question 7: Peer to Peer file sharing. Answer either “Yes” or “No”. Per ASD(NII)/DoD CIO Memorandum, “Use of Peer-to-Peer (P2P) File-Sharing Applications across DoD,” dated November 23, 2004, P2P file-sharing is an information technology that permits computer users to share files with other users without centralized security controls or oversight. DoD Components are encouraged to identify and eliminate unauthorized P2P file-sharing activities originating in or traversing their networks. As part of this effort, IA awareness training addresses unauthorized P2P file-sharing on DoD systems. DoD Components shall comply with this guidance.

c. Question 8: Configuration Management. The narrative of this response will specifically address the extent to which Components are compliant to all applicable Security Technical Implementation Guides (STIG) and OMB-mandated configuration policies, e.g. Federal Desktop Core Configuration (FDCC) for Windows XP and Vista Operating Systems.

(1) Question 8.a. will be answered by OSD.

(2) Question 8.b. is to be answered by the Component. This question deals with to what extent STIGs are implemented on systems in general.

4. SECTION B OMB TEMPLATE, QUESTIONS 9, 10, AND 11

a. Questions 9.a. and 9.b. are to be completed by Components.

b. Question 9.c. is to be completed by USSTRATCOM based on information provided by JTF-GNO IAW their Unified Command Plan Computer Network Defense Mission.

c. Questions 10.a. and 10.b. will be completed by OSD.

d. Question 11 will be completed by OSD.

<b>Section B - Chief Information Officer: Questions 9, 10, and 11</b>									
<b>Agency Name:</b>									
<b>Question 9: Incident Reporting</b>									
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.									
9.a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.									
9.b. The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. ( <a href="http://www.us-cert.gov">http://www.us-cert.gov</a> )									
9.c. The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.									
Comments:									
<b>Question 10: New Technologies and Emerging Threats</b>									
10.a. Has the agency documented in its security policies, special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)? Yes or No.									
10.b. If the answer to 10 a. is "Yes," briefly describe the documented procedures. These special procedures could include more frequent control tests & evaluations, specific configuration requirements, additional monitoring, or specialized training. Response:									
<b>Question 11: Performance Metrics for Security Policies and Procedures</b>									
Please describe three (3) performance metrics your agency uses to measure the effectiveness or efficiency of security policies and procedures. The metrics must be different than the ones used in these FISMA reporting instructions, and can be tailored from NIST's Special Publication 800-80 "Guide for Developing Performance Metrics for Information Security."									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; text-align: center;">Performance Metric Name</th> <th style="width: 50%; text-align: center;">Description</th> </tr> </thead> <tbody> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </tbody> </table>	Performance Metric Name	Description							
Performance Metric Name	Description								

**Figure 5. OMB Template, Section B, Questions 9, 10, and 11**

(INTENTIONALLY BLANK)

## ATTACHMENT 3

### COMPLETION OF DITPR AND SIPRNET IT REGISTRY FIELDS

1. BACKGROUND. This attachment provides guidance on completing the DoD Information Technology Portfolio Repository (DITPR) fields used for quarterly and annual FISMA reports to OMB and Congress.

a. The data fields specifically reviewed and used for FISMA FY08 reporting are outlined below.

b. The answers to these fields are based on required documentation (e.g., accreditation decision, Information Technology (IT) Contingency Plan (CP), IT Security Plan of Action and Milestones (POA&M), etc.) The documentation is subject to review and auditing.

### 2. FIELDS USED FOR FISMA REPORTING

#### a. Certification and Accreditation (C&A) Field

(1) The "Security Certification and Accreditation Required" field is mandatory for all registered systems and is the first FISMA field that should be completed.

(2) Determine if the system requires accreditation (e.g., DoD Information Assurance Certification and Accreditation Process (DIACAP) or for intelligence systems IAW DCID 6/3) and provide one of the two following answers in the registry (Figure 1).

(3) Answers:

(a) **Yes**. An answer of "Yes" means the system requires accreditation IAW certification and accreditation (C&A) guidance **AND** is operational.

(b) **No**. An answer of "No" means the system does not require certification and accreditation or the system is currently not operational (e.g., pre-deployment). An answer of "no" requires an explanation in the "Accreditation Not Required Explanation" field (see paragraph 3.b. below). This includes systems that are "not operational" due to a Denial of Authorization to Operate (DATO) accreditation decision. Systems with an IATT are not operational and should also answer "No".

(4) Examples as they apply to IT Platform or Interconnection components:

(a) IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.) – Accreditation Required Answer: “No”

(b) IT which is integral to real-time execution of the platform mission (e.g., sensor-to-processor links, radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems) – Accreditation Required Answer: “No”

(c) IT that is part of or connected with the platform that also connects to external applications that process data in support of the platform (e.g., logistics, training, scheduling, remote diagnostics, etc.) – Accreditation Required Answer: “Yes”

(d) IT that is part of or connected with the platform that is part of a defined Information Exchange Requirement (IER) or interfaces with the Global Information Grid (GIG) – Accreditation Required Answer: “Yes”

b. Accreditation Not Required Explanation Field

(1) The "Accreditation Not Required Explanation" field is mandatory for all registered systems that answered "No" in the "Security Certification and Accreditation Required" field.

(2) If the system does not require certification and accreditation provide one of the five following answers in the registry (Figure 1).

(a) **Embedded IT.** An answer of “Embedded IT” means IT is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.). **STOP - DO NOT COMPLETE ANY FURTHER FISMA FIELDS.**

(b) **Integral to real-time execution.** An answer of “Integral to Real-Time Execution” mean IT is integral to real-time execution of the platform mission (e.g., radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility Supervisory Control and Data Acquisition (SCADA) systems). **STOP - DO NOT COMPLETE ANY FURTHER FISMA FIELDS.**

(c) **Without platform interconnection.** An answer of “Without Platform Interconnection” means IT does not communicate outside the platform. STOP - DO NOT COMPLETE ANY FURTHER FISMA FIELDS.

(d) **Pre-Deployment.** An answer of “Pre-Deployment” means IT requires C&A but is still in one of the developmental stages (Concept Refinement, Technology Development, System Development & Demonstration) of its life cycle. Ensure life cycle (LIFE CYCLE field in Core area) reflects correct stage (Concept Refinement, Technology Development, System Development & Demonstration). STOP - DO NOT COMPLETE ANY FURTHER FISMA FIELDS.

(e) **IATT.** Interim Authorization to Test (IATT) means a temporary Designated Accrediting Authority (DAA) authorization to test a system in a specified information environment within the timeframe and under the conditions or constraints enumerated in the accreditation decision. The IATT requires documentation of the accreditation decision. See DoDI 8510.01 (DIACAP) for further guidance. STOP - DO NOT COMPLETE ANY FURTHER FISMA FIELDS

(f) **DATO.** An answer of “DATO” (Denial of Authorization to Operate) means that the DAA determined that a system can not operate because of an inadequate IA design or failure to implement assigned IA controls, or it has been decommissioned. The answer requires documentation. If a system is already operational, the operation of the system is halted. If the system has been decommissioned it should be archived in DITPR. STOP - DO NOT COMPLETE ANY FURTHER FISMA FIELDS.

(3) Note: IATT and DATO are accreditation decisions per DIACAP and reflect an accreditation status. However, **systems in this status are not operational** and, therefore, not reported for FISMA purposes.

c. Information Assurance Record Type Field

(1) The "Information Assurance Record Type" field is mandatory for all registered systems that answered "Yes" to the "Security Certification and Accreditation Required" field. (Figure 2)

(2) Determine the IA Record Type of the system and provide one of the four following answers in the registry.

(a) **Application.** An answer of “Application” (automated information system (AIS) application) means the application (system) is either the product or deliverable of

an acquisition program, such as those described in DoD Directive 5000.1 or a DoD internally-developed system or application.

1. An AIS, per DoDI 8500.2, is analogous to OMB A-130 definition of a “major application,” which means one that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

2. An application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)).

(b) **Enclave.** An answer of “Enclave” means the collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

(c) **Out-Sourced IT-based Process.** An answer of “Outsourced IT-based Process” means the system is an outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services.

(d) **Platform IT Interconnections.** An answer of “Platform IT Interconnections” means a system with network access to the platform IT. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the performance of special purpose systems.

1. Examples of these systems include weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric.

2. Examples of platform IT interconnections that impose security considerations include: communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote reconfiguration.

d. Mission Assurance Category (MAC) Field

(1) The "Mission Assurance Category" field is mandatory for all registered systems that answered "Yes" for the "Security Certification and Accreditation Required" field (Figure 2).

(2) Determine the MAC of the system and provide one of the three following answers in DITPR or the SIPRNET IT Registry (Note: IAW DoDI 8500.2, "Information Assurance (IA) Implementation," dated February 6, 2003, "Heads of DoD Components shall: Assign mission assurance categories to DoD component-specific DoD information systems according to the guidelines provided in enclosure 4 of this Instruction").

(a) **MAC I.** An answer of "MAC I" means a system handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

(b) **MAC II.** An answer of "MAC II" means a system handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

(c) **MAC III.** An answer of "MAC III" means a system handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

(3) Note: The Mission Criticality and MAC are two separate designations and do not necessarily correspond one for one in each of three levels. For example: A system could be designated as MC and MAC II or ME and MAC I. A financial system could be designated MC (by USD(C)) and MAC III (by DoD Component), however in most other cases the designation of a systems as MC and MAC III is unusual and should be reviewed

closely prior to making this designation combination. (Note: more detailed discussion on mission criticality can be found in section 4, paragraph a below.)

e. Confidentiality Level Field

(1) The "Confidentiality Level" field is mandatory for all registered systems that answered "Yes" for the "Security Certification and Accreditation Required" field (Figure 2).

(2) The confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). DoD has three defined confidentiality levels: classified, sensitive, and public.

(3) Determine the confidentiality level of the system and provide one of the three following answers in registry:

(a) **Public.** An answer of "Public" means the system contains information that has been cleared to be released to the public.

(b) **Sensitive.** An answer of "Sensitive" means system contains sensitive information (see DoDI 8500.2 definition).

(c) **Classified.** An answer of "Classified" means system contains classified information.

f. Accreditation Vehicle Field

(1) The "Accreditation Vehicle" field is mandatory for all registered systems that answered: "Yes" for the "Security Certification and Accreditation Required" field (Figure 2).

(2) Determine the certification and accreditation (C&A) process used to grant the current system accreditation and provide one of the five following answers in the registry.

(a) **DITSCAP.** An answer of "DITSCAP" means the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) was used to conduct system certification and make an accreditation decision.

(b) **DIACAP.** An answer of “DIACAP” means the DoD Information Assurance Certification and Accreditation Process (DIACAP) was used to conduct system certification and make an accreditation decision.

(c) **DCID 6/3.** An answer of “DCID 6/3” means the Director of Central Intelligence Directive (DCID) 6/3 was used to conduct system certification and make an accreditation decision.

(d) **NIST SP 800-37.** An answer of "NIST SP 800-37" means that the National Institute of Technology (NIST) SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" was used to conduct system certification and make an accreditation decision. A system that has been designated as a National Security System (NSS) cannot be accredited under NIST SP 800-37.

(e) **NISPOM.** An answer of "NISPOM" means the National Industrial Security Program Operating Manual (NISPOM) was used to conduct system certification and make an accreditation decision.

g. Accreditation Status Field

(1) The "Accreditation Status" field is mandatory for all registered systems that answered "Yes" for the “Security Certification and Accreditation Required” field (Figure 2).

(2) Determine accreditation status of the system and provide one of the following answers:

(a) **ATO.** Answer of “ATO” (Authorization to Operate) means authorization, granted by a DAA, for a system to process, store or transmit information. Authorization is based on the acceptability of the IA Component, the system architecture and implementation of assigned IA controls. The answer requires documentation of completed certification and accreditation process and accreditation decision. Complete the fields listed in Figure 3.

(b) **IATO.** Answer of “IATO” (Interim Authorization to Operate) means a temporary DAA authorization to operate a system under conditions or constraints enumerated in the accreditation decision. The answer requires documentation of completed certification and accreditation process, accreditation decision, and plan of actions and milestones (POA&M) to resolve security weaknesses that prevented the granting of an ATO. Complete the fields listed in Figure 3.

(c) **NONE.** Answer of “None” means the system requires Security Certification and Accreditation and is operational, but does not have a current accreditation. Complete the fields listed in Figure 3.

(3) Note: When changing “Security Certification and Accreditation Required” field from “No” to “Yes”, complete the required fields in Figures 2 and 3.

h. Accreditation Date Field

(1) Determine the date authorization granted by the DAA.

(2) Complete field with date authorization granted by the DAA.

(3) If an accreditation status of ATO or IATO is selected, then accreditation date field is mandatory.

(4) If a system does not have an accreditation decision of ATO or IATO leave the accreditation date field blank.

**(5) Future dates are not permitted for the accreditation date field, nor will the DITPR accept them.**

i. Accreditation Expiration Field

(1) If an accreditation status of ATO or IATO is selected, the accreditation expiration field is mandatory and must match the accreditation documentation.

(2) The ATO expiration date cannot exceed 3 years from the authorization date. For example, if the authorization date of an ATO is 20060521 the expiration date cannot be later than 20090520.

(3) The IATO expiration date cannot exceed 180 days from the authorization date. For example, if the authorization date of an IATO is 20050501 the expiration date cannot be later than 20051027 (180 days). A DAA may not normally grant consecutive IATO's totaling more than 360 days. See DoDI 8510.01 (DIACAP) for further guidance.

(4) If a system does not have an ATO or IATO, leave the expiration date field blank.

j. Security Control Test Field

(1) Determine the date system security controls completed testing. The date should be derived from either:

(a) The date system security controls completed testing for certification recommendation prior to accreditation decision or;

(b) The date system security controls testing completed prior to or during annual security review. System security controls must be tested within a 12 month period IAW with DoDI 8500.2 (see Attachment 2, paragraph 2 – Mandatory System Control Testing) or due to changes in the system IA controls that bring those controls out of compliance with DoD requirements and/or the DAA accreditation decision.

(2) Enter the date of the most recent security control testing completed.

**(3) Future dates are not acceptable for security control testing completed field, nor will the DITPR accept them.**

(4) For a system that has never had security controls tested leave field blank.

k. IT Contingency Plan Field

(1) DoD mission critical, mission essential and mission support systems must complete this field.

(2) Determine if the system has a written and approved IT contingency plan in place to provide interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods. Provide one of the two following answers in the registry.

(a) **Yes.** An answer of “Yes” means the system has a written and approved IT contingency plan.

(b) **No.** An answer of “No” means the system does not have a written and approved IT contingency plan.

(3) A system may have a separate IT contingency plan or be included in a larger contingency plan. For example, an AIS application (system) may be included within an enclave IT contingency plan. In this case the enclave plan must explicitly document inclusion of the AIS application and include system-specific caveats. The Program Manager (PM) over the system should collaborate closely with the CIO, enclave PM, and other system PMs to assure an adequate CP.

(4) Type accredited systems may have a system specific IT contingency plan and/or a baseline IT contingency plan providing guidance to deployed locations (e.g., enclaves).

1. IT Contingency Plan Tested Date Field

(1) Determine if the IT contingency plan has been tested.

(a) Systems for which the answer “Yes” was entered under the "IT Contingency Plan" field will enter the most current contingency plan test date.

**1. Future dates are not acceptable for contingency plan test date, nor will the DITPR accept them.**

2. If the system does not have an IT contingency plan test date leave the date field blank.

(b) Systems for which the answer “No” was entered under the IT Contingency Plan” field are not permitted to enter contingency plan test date.

(2) Guidance on contingency plan testing can be found in attachment 5.

m. IT Security Plan of Action and Milestones (POA&M) Operating with An Open Weakness Field (Change)

(1) Determine if the system requires an IT Security POA&M due to unresolved security weaknesses and provide one of the two following answers in the registry.

(a) **Yes.** An answer of “Yes” means there is an IT Security POA&M for the system with an open weakness.

(b) **No.** An answer of “No” means the system does not currently have an IT Security POA&M with an open weakness.

(2) The primary purpose of an IT Security POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities.

(a) OMB requires agencies to prepare POA&Ms for all programs and systems in which an IT security weakness has been found. OMB guidance directs CIOs and the DoD Component program officials to develop, implement, and manage IT Security POA&Ms for all programs and systems they operate and control (for program officials this includes all systems that support their operations and assets, including those operated by contractors).

(b) In addition, program officials are required to update the agency CIO on their progress on at least a quarterly basis and at the direction of the CIO. This enables the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB for MAC I and II systems. For instructions on completing a POA&M see Attachment 7 of this guidance and for an in-depth discussion of the actual POA&M process, refer to DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)".

(3) Note: The purpose of this field has changed from identifying whether a POA&M is required for a system to whether currently there is a POA&M with an open unresolved weakness for this systems. The POA&M date submitted field will be deleted and does not need to be completed.

(4) A system operating under an IATO is required to have an IT Security POA&M. An answer of "No" in this field for a system operating under an IATO will be a "Red Flag" for inspection or auditing, since the issuance of IATO implies open weaknesses.

n. System Operating with One or More Security Weaknesses That Are Greater than 120 Days Beyond the Planned Remediation Date in the POA&M Field (New Field)

(1) If an answer of "Yes" is provided in the IT Security POA&M field, then answering this field is **mandatory**.

(2) Answering "Yes" indicates there are one or more weaknesses open and are more than 120 past the planned remediation date.

(3) Answering “No” indicates there are open weaknesses that are 120 days or less past the planned remediation date and the answer to paragraph o below will be “Yes”.

(4) Note: To avoid getting penalized twice when reporting these metrics to OMB, if this answer is “Yes”, DITPR will **not** allow the question for 90-120 days (paragraph o below) to also be “Yes”. This is done to prevent double counting of any one system with the intent to show systems in the “category representing the most overdue security weakness.” Table 1 is provided to clarify this relationship.

Weakness?	Over 120 Days	90 - 120 Days	Comments
Yes	No	No	Weaknesses <i>less than 90 days</i>
Yes	Yes	No	Prevents double counting
Yes	No	Yes	Prevents double counting
Yes	Yes	Yes	NOT PERMITTED
No	n/a	n/a	Subsequent fields not triggered

**Table 1: POA&M Status Matrix**

(5) This field will be used for quarterly and annual FISMA reporting.

(6) OASD(NII) will establish the report as of date. For example: The report date is 13 February 2008. A weakness will be counted, if the system is operating with a weakness that had a planned remediation date **originally** scheduled for completion on or before 15 October 2007.

(7) This field is being created to meet OMB reporting requirements. The addition of this field will eliminate the need for separate data call to the DoD Components each quarter.

o. Is the System Operating with One or More Security Weaknesses That Are 90-120 Days Beyond the Planned Remediation Date in the POA&M Field (New Field)

(1) If an answer of “Yes” is provided in the IT Security POA&M field, then answering this field is **mandatory**.

(2) Answering “Yes” indicates there are one or more weakness open and between 90 and 120 past the planned remediation date.

(3) Answering “No” indicates there are open weaknesses that are less than 90 days or more than 120 days past the planned remediation date.

(4) This field will be used for quarterly and annual FISMA reporting.

(5) OASD(NII) will establish the report as of date. For example: The report date is 13 February 2008. A weakness will be counted if the system is operating with a weakness that had a planned remediation date **originally** scheduled for completion between 14 October and 15 November 2007.

(6) This field is being created to meet OMB reporting requirements. The addition of this field will eliminate the need for separate data call to the DoD Components each quarter.

p. Annual Security Review Date.

(1) Determine the date an annual security review required by FISMA and DoD was completed.

(a) If an information system has had an accreditation decision within *12 months for an authorization to operate (ATO)* or *180 days for an interim authorization to operate (IATO)* enter the accreditation decision date within the annual information system review date. This constitutes a valid annual information system review.

(b) If the information system has not had an accreditation decision, ATO (within 12 months) as of 1 October of the Fiscal Year then an information system review (assessment) will be required.

(2) Program officials are responsible for reviewing the security of all systems under their respective control.

(3) The necessary depth and breadth of an annual system review depends on several factors such as:

(a) Potential risk and magnitude of harm to the system or data;

(b) Relative comprehensiveness of last year's review; and

(c) Adequacy and successful implementation of security controls and the IT Security POA&M for weaknesses in the system.

(4) If last year a system underwent a complete C&A, this year a relatively simple update or maintenance review may be sufficient, **provided it has been adequately documented within the agency**. At a minimum, agency officials and CIOs must take

into account the three criteria listed above in determining the appropriate level of annual review of system security controls (see attachment 4 below).

- (a) Enter the date last annual review completed;
- (b) Enter an accreditation decision date for ATO within 12 months; or
- (c) Enter an accreditation decision date for IATO within 180 days.

**(d) Future dates are not acceptable for annual security review date field, nor will the DITPR accept them.**

(e) For a system that has not completed the annual security review, leave the field blank.

#### 4. CORE FIELDS USED FOR FISMA REPORTING

a. Mission Criticality Field. Determine mission criticality of the system and provide one of the three following answers in the registry.

(1) An answer of “MC” (Mission Critical) means system meets the definitions of “information system” and “national security system” in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: Designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller), (USD(C)). A “Mission-Critical Information Technology System” has the same meaning as a “Mission-Critical Information System.” DoDI 5000.2, May 12, 2003.

(2) An answer of “ME” (Mission Essential) means the system meets the definition of “information system” in the Clinger-Cohen Act, that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(C)). A “Mission-Essential Information Technology System” has the same meaning as a “Mission-Essential Information System.” DoDI 5000.2, May 12, 2003.

(3) An answer of “MS” (Mission Support) means the system is neither Mission Critical nor Mission Essential.

b. System Operation Field. Determine the appropriate category and provide one of the five following answers in the registry.

(1) **GOGO**. An answer of “GOGO” means the system is Government (DoD) Owned and Government Operated. **A system that has contractor support integrated with government personnel to operate the system is government operated.**

(2) **GOCO**. An answer of “GOCO” means the system is Government (DoD) Owned and Contractor Operated (GOCO).

(3) **COCO**. An answer of “COCO” means the system is Contractor Owned and Contractor Operated (COCO). This includes contracted outsourced IT services and processes performed on the behalf of the Department of Defense and DoD Component sponsored contractor enclave connected to DoD networks (e.g., SIPRNET and NIPRNET).

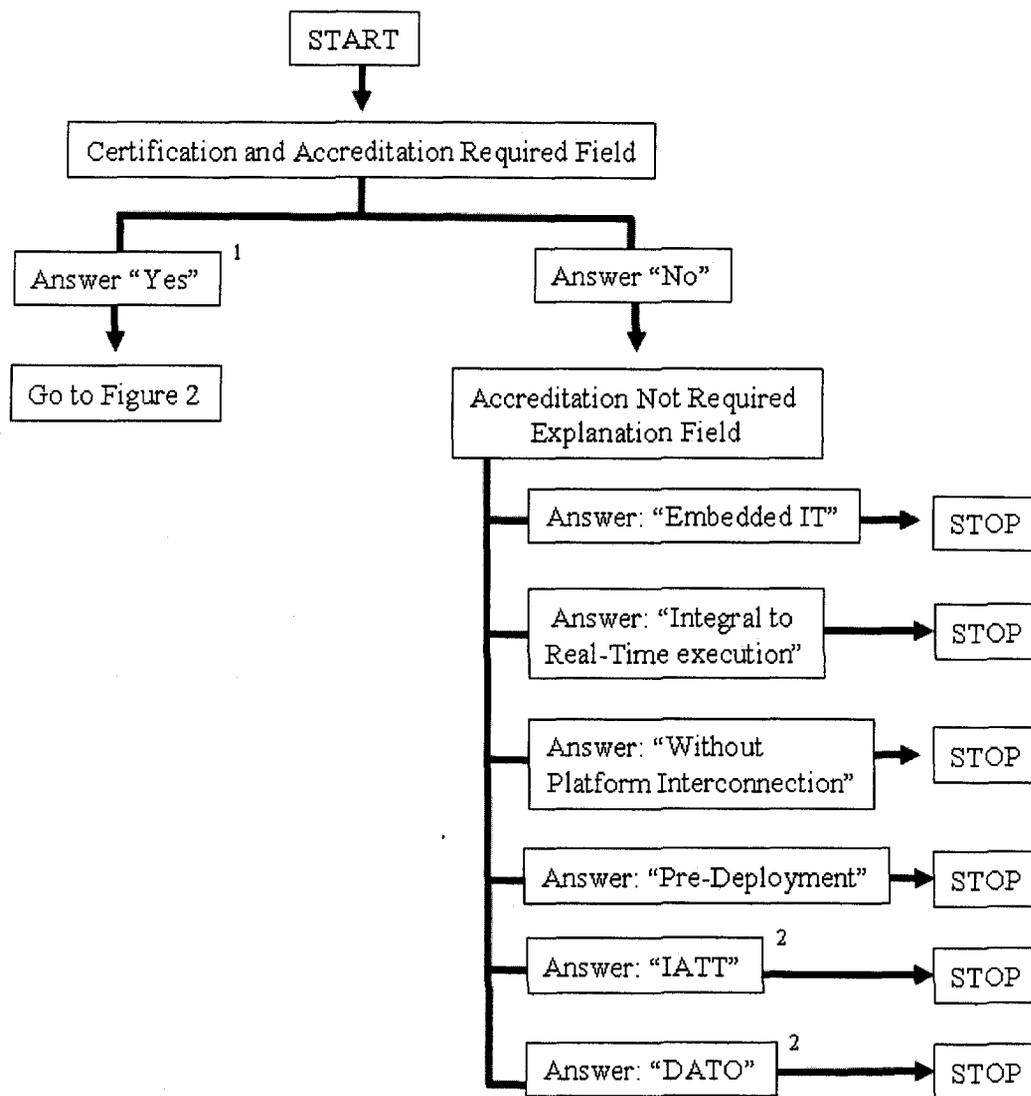
(4) **COGO**. An answer of “COGO” means the system is Contractor Owned and Government (DoD) Operated (COGO).

(5) **Non-DoD**. An answer of “Non- DoD” means Federal, State and local governments, grantees, and industry partner systems are connected to DoD information systems and have access to DoD information. **Systems in this category should not be reported by DoD Components under FISMA.**

5. COMPLIANCE VERIFICATION. As indicated in paragraph 1.b above, source documentation for repository data are subject to verification and auditing. The DoD CIO Compliance Program (DCCP) is undertaken as part of the DoD CIO’s responsibility to oversee and verify Component compliance with Federal IT security regulations and DoD IA policy.

a. It consists of three levels of assessment: 1) repository data accuracy review; 2) documentation and artifacts request and review; then, 3) on-site verification review at Component locations, if needed, to verify documentation and compliance status.

b. Findings from the three reviews will allow the DoD CIO to make a determination of Component compliance with the requirements of FISMA and other OMB reporting.



Notes:

<sup>1</sup> An answer of "Yes" means **system requires C&A and is operational**.

<sup>2</sup> IATT and DATO are accreditation decisions and reflect an accreditation status. However, **systems in this status are not operational** and are not reported for FISMA.

Figure 1. Certification and Accreditation Required Field

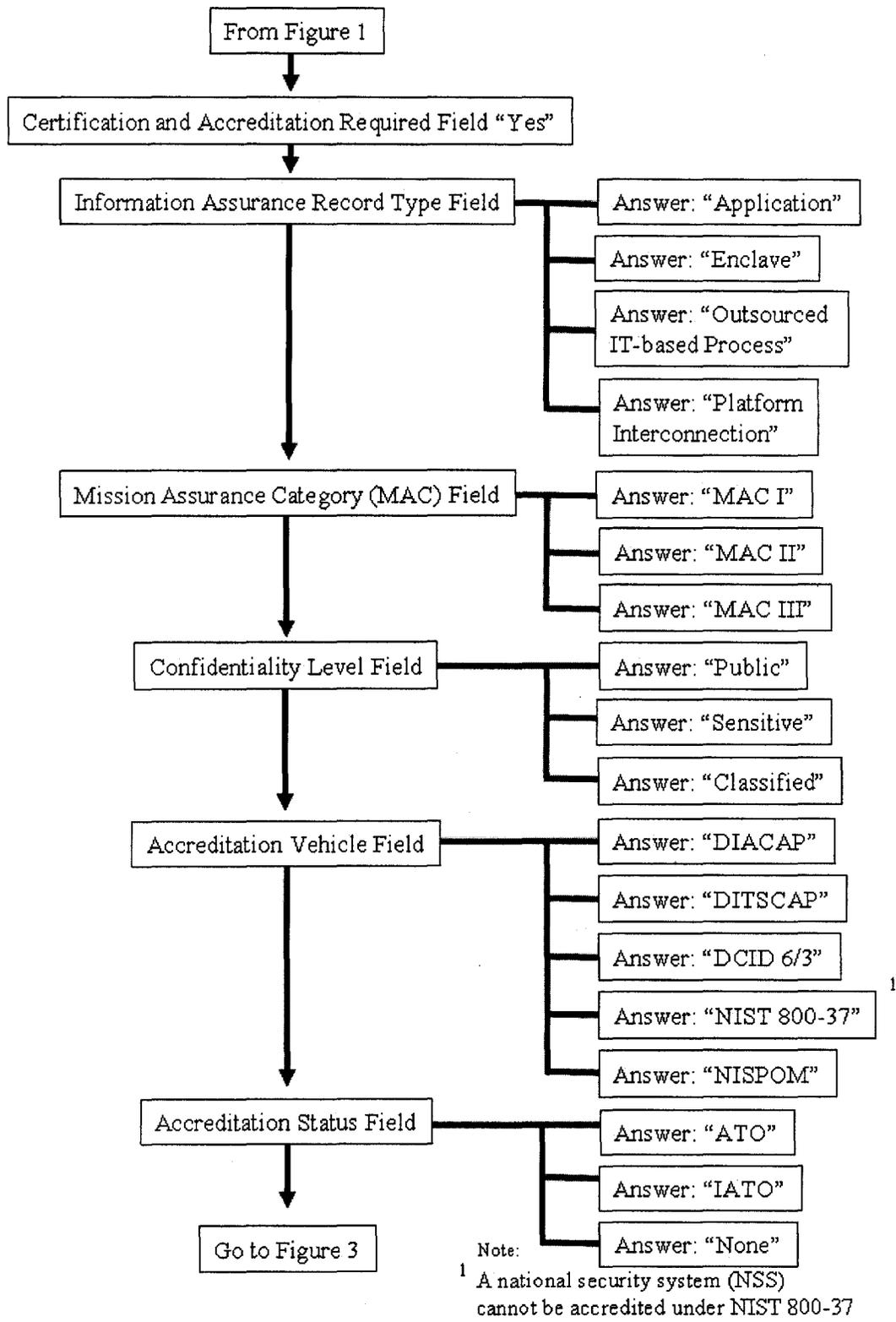


Figure 2. Certification and Accreditation Required "Yes" Fields

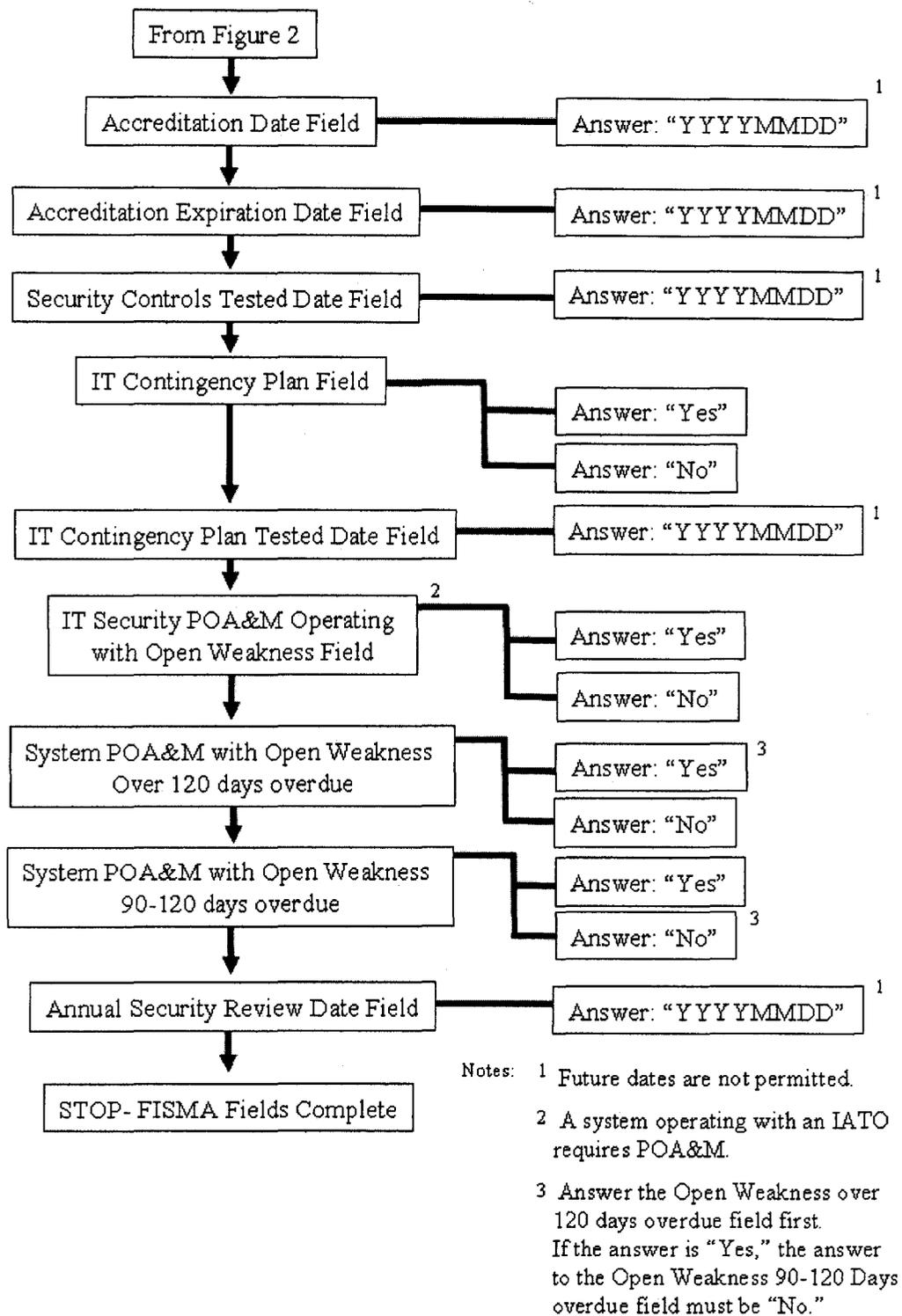


Figure 3. Certification and Accreditation Required "Yes" Fields

(INTENTIONALLY BLANK)

## ATTACHMENT 4

### ANNUAL SECURITY REVIEW AND IA CONTROLS TESTING REQUIREMENTS

1. INTRODUCTION. This attachment provides guidance to assist in completing an Annual Security Review and required security controls testing as required by FISMA and DoD Directive 8500.01E, “Information Assurance (IA)”. Primary instructions for implementation, review, and testing of these are provided in:

- a. DoDI 8500.2, “Information Assurance (IA) Implementation”.
- b. DoDI 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP)”, dated November 28, 2007.

### 2. MANDATORY IA (SECURITY) CONTROLS TESTING

a. DoD Instruction 8500.2 requires periodic testing for the following IA controls:

- (1) COED-2 Scheduled Exercises and Drills – Semi-Annual. The continuity of operations or disaster recovery plans, or significant portions, are *exercised semi-annually*. Disaster recovery procedures include business recovery plans, IT contingency plans, facility disaster recovery plans, and plan acceptance. (Applies to MAC I systems)
- (2) COED-1 Scheduled Exercises and Drills – Annual. The continuity of operations or disaster recovery plans are *exercised annually*. (Applies to MAC II and III systems)
- (3) DCAR-1 Procedural Review – Annual. An *annual IA review* is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.
- (4) DCSS-2 System State Changes – Periodic. System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. *Tests are provided and periodically run to ensure the integrity of the system state.*

- (5) ECPC-2 Production Code Change Controls – Quarterly. Application programmer privileges to change production code and data are limited and *reviewed every 3 months*. (Applies to MAC I and MAC II systems)
- (6) ECPC-1 Production Code Change Controls – Periodic. Application programmer privileges to change production code and data are limited and *are periodically reviewed*. (Applies to MAC III systems)
- (7) VIIR-2 Incident Response Planning – Semi-Annual. An incident response plan exists that identifies the responsible Computer Network Defense (CND) Service Provider IAW DoD Instruction O-8530.2. It defines reportable incidents, outlines a standard operating procedure for incident response to include the information operations condition (INFOCON), provides for user training, and establishes an incident response team. *The plan is exercised at least every 6 months*. (Applies to MAC I systems)
- (8) VIIR-1 Incident Response Planning – Annual. An incident response plan exists that identifies the responsible CND Service Provider IAW DoDI O-8530.2. *The plan is exercised at least annually*. (Applies to MAC II and MAC III systems)

b. Reminder: The COED controls test date is reported separately in the IT Contingency Plan Test field of the DoD SIPRNET IT Registry for FISMA reporting.

### 3. ANNUAL SYSTEM SECURITY REVIEW

a. DoD Component systems must meet the security controls in DoDI 8500.2. Annual reviews examine, review, and test the implementation of assigned system security controls as appropriate.

b. NOTE: An example of an annual review form is provided in Annex A for discussion of the annual review process and to show scope. DoD components or organizations may use different review forms or automated processes to complete the annual review of controls.

c. System Review Requirements and Currency

(1) If an information system has had an accreditation decision within *12 months for an authorization to operate (ATO) or 180 days for an interim authorization to operate (IATO)* enter the accreditation decision date within the annual information system review date field. This constitutes a valid annual information system review.

(2) If the information system has not had an accreditation decision, ATO (within 12 months) or IATO (within 180 days) an information system review (assessment) will be required.

d. Annual Information System Review Documentation

(1) This paragraph provides instruction on completing the System Reporting Form cover sheet (see Annex A: Annual Information System Review cover sheet below), standardizing how the completed evaluation should be marked, how systems are titled, and assigning/documenting the Mission Assurance Category and Confidentiality Level of the system.

(a) System Identification. The cover page of the System Reporting Form cover sheet (see Annex A: Annual Information System Review cover sheet below) begins with the name and acronym and unique identifier of the system to be assessed.

(b) Type of System. Assign the system category as application, enclave (which includes networks), outsourced IT-based processes or platform IT interconnections IAW DoD Directive 8500.1, Information Assurance (IA).

(c) Mission Assurance Category (MAC). Assign the applicable Mission Assurance Category (MAC) as either:

1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or

degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

(d) Confidentiality Level. Assign the confidentiality level as Classified, Sensitive or Public.

(e) Accreditation Date. The date an accreditation decision was made approving the operation of the system.

(f) Connected Systems. The connected systems should be listed, along with the date when the system was certified and accredited. Example: Enclave within which an application is operating. Network connection (e.g., NIPRNET or SIPRNET).

(g) Purpose of Assessment. The purpose and objectives of the assessment should be identified. For example, the assessment may have been performed to satisfy the annual FISMA reporting requirement, to document a C&A, to assess the security posture of a system after changes have been made, or to document the continuous monitoring of a system.

(h) Assessor Information. The name, title, and organization of the individuals who perform the assessment.

(i) Assessment Date. Date the assessment was completed.

(2) There are eight control subject areas in the System Reporting Form. Each control subject area, and its respective set of controls, is identified in this guidance exactly as they are documented in DoDI 8500.2. For example, the identifier for the Security Design and Configuration subject area is DC; the identifier for the Enclave Boundary Defense is EB.

(3) Each control subject area is comprised of a number of controls. Some control subject areas have as few as three controls while others as many as 48. In the System Reporting Form, each subject area has its own section and within each section, each control has a row in which the results of the assessment are to be documented.

(4) The selection of baseline controls is based on the MAC (i.e., MAC I, MAC II and MAC III) and Confidentiality Level (Public, Sensitive and Classified assigned to the system. A DAA can direct additional controls be integrated into a system and these controls would be added to the C&A and would then continue to be reviewed annually.

4. ANNUAL REVIEW OF SYSTEM CONTROLS. In completing the System Reporting Form (see example Annex A below), each control for a system is reviewed and answered.

a. Control Implemented Correctly & Completely (Valid). Includes the determination that the Security control is implemented correctly and completely IAW with implementation plan and accreditation decision. Answers choices are:

(1) **Yes**. An answer of “YES” means the information security control is implemented correctly and effectively in a consistent manner. This also means that testing was conducted during certification to ensure controls will operate as intended and continue to operate as intended.

(2) **Inherited**. An answer of “Inherited” means the information security control has been inherited from another system. For example, the security control for an application is inherited from the implementation of a security control in an enclave in which it is deployed.

(3) **No**. An answer of “NO” means the information security control is not fully implemented. This can mean the DAA has accepted risk for not implementing a control or partially implementing a control.

(4) **NA**. An answer of “NA” means the information security control is not applicable to the system based on MAC and/or confidentiality level as a baseline control and was not selected as an additional control by the DAA. The sample form can be modified by deleting rows for those controls that are not applicable.

b. Risk Accepted or Control Not Fully Implemented. Includes the determination that the DAA accepted risk by not implementing security control and/or partially implemented security control. Answer choices are:

(1) **Partial**. An answer of “Partial” means the information security control is partially implemented and the DAA has accepted the risk. This also means that a weakness for the control will be listed on the system IT Security POA&M.

(2) **Risk Accepted**. An answer of “Risk Accepted” means the information security control has not been implemented and the DAA has accepted the risk. This also means that a weakness for the control will be listed as a weakness on the system IT Security POA&M.

c. Weakness Listed on System IT Security POA&M and/or Mitigated. Includes the determination that the Security control is **not** implemented correctly and completely IAW with implementation plan and accreditation decision. Answer choices are:

(1) **POA&M**. An answer of “POA&M” means the weakness caused by or tied to the security control is documented on the system IT Security POA&M. The IT Security POA&M must be available for review.

(2) **Mitigated**. An answer of “Mitigated” means the weakness caused by or tied to the security control is documented on the system IT Security POA&M. In addition, the organization has implemented actions to mitigate the weakness.

d. Control Evaluated or Tested in Last 12 Months. Includes determination that the security control has been evaluated or tested IAW DoD Instruction 8500.2 and DoD guidance related to the security control. Answer choices are:

(1) **1 Time**. An answer of “1 Time” means for a system that a security control has been evaluated or tested once during previous 12 months to ensure they are operating as intended or due to changes in system – that IA controls are in compliance with DoD requirements and/or DAA accreditation decision and tests have been conducted to ensure they are operating as intended. Ensured that effective corrective actions are taken to address identified weaknesses (i.e., IT Security POA&M), including those identified as a result of potential or actual security incidents or through security alerts issued by federal organizations, vendors, and other trusted sources.

(2) **2+ Times**. An answer of “2+ Times” means for a system that security control has been evaluated or tested two or more times during the previous 12 months to ensure they are operating as intended or due to changes in system – that IA controls are in

compliance with DoD requirements and/or DAA accreditation decision and tests have been conducted to ensure they are operating as intended. Ensured that effective corrective actions are taken to address identified weaknesses (i.e., IT Security POA&M), including those identified as a result of potential or actual security incidents or through security alerts issued by federal organizations, vendors, and other trusted sources. Certain controls are required to be evaluated or tested periodically or more than once each year.

(3) **No.** An answer of “NO” means for a system that a security control has not been evaluated or tested in the previous 12 months.

e. Review Form. To assist in completing review and reduce the length of time to complete an annual review it is recommended that a review form be maintained during an annual cycle and as controls are exercised or tested the review be updated. Examples:

(1) CP is exercised therefore the annual review form and continuity (CO) and other CP-related controls exercised could be updated with the date of test.

(2) Physical and environmental controls (PE) could be updated with test dates for such controls as fire inspection (PEFI-1), physical security testing (exercise) (PEPS-1) and visitor control (PEVC-1).

(3) Vulnerability management (VIVM-1) use of vulnerability assessment and management tools (scanning).

(4) User accounts are periodically reviewed to ensure only authorized user accounts are active (IAAC-1) and users are logging on properly in compliance with organization guidance (IAIA-1).

f. Sufficiency of Scope. Reviews of documentation, walk-through of agency facilities, and interviews with agency personnel, while providing useful information, are not sufficient to ensure that controls, especially technical controls, are operating effectively.

(1) Examples of evaluation or tests that can be conducted:

(a) Network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing).

(b) Evaluations of procedures or plans in tabletop or functional exercises can also be conducted. See attachment 5 for more discussion of tabletop and functional exercises in context of contingency plans.

(2) When systems are first implemented or are modified, they are tested and certified to ensure that the security controls are operating as intended.

g. Date of Last Test(s) – includes the determination of dates in previous 12 months when evaluation or tests were conducted for the security controls. Answers include:

(1) One date or multiple dates may be recorded to account for those controls completing more than one evaluation or test within 12 month period.

(2) Leaving the field as “YYYY/MM/DD” means that no evaluation or test was conducted in previous 12 months.

Annex A: Annual Information System Review

1. System Identification:

Name: \_\_\_\_\_

Acronym: \_\_\_\_\_

Unique Identifier: \_\_\_\_\_

2. Type of System:

\_\_\_\_\_ Application

\_\_\_\_\_ Enclave

\_\_\_\_\_ Outsourced IT-based Process

\_\_\_\_\_ Platform IT interconnection

3. Accreditation Date: \_\_\_\_\_

4. Connected Systems: \_\_\_\_\_  
\_\_\_\_\_

5. Mission Assurance Category (MAC):

\_\_\_\_\_ MAC I

\_\_\_\_\_ MAC II

\_\_\_\_\_ MAC III

6. Confidentiality Level:

\_\_\_\_\_ Classified

\_\_\_\_\_ Sensitive

\_\_\_\_\_ Public

7. Purpose of the Assessment: \_\_\_\_\_  
\_\_\_\_\_

8. Name of Assessors:

a. \_\_\_\_\_

b. \_\_\_\_\_

c. \_\_\_\_\_

9. Date of Assessment: \_\_\_\_\_

1. Continuity Controls

Security Controls (Continuity)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M and/or Mitigated	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
COAS-2 Alternate Site Designation MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COAS-1 Alternate Site Designation MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COBR-1 Protection of Backup and Restoration Assets MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
CODB-3 Data Backup Procedures MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
CODB-2 Data Backup Procedures MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
CODB-1 Data Backup Procedures MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
CODP-3 Disaster and Recovery Planning MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
CODP-2 Disaster and Recovery Planning MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Continuity)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s)  YYYY/MM/DD
CODP-1 Disaster and Recovery Planning  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COEB-2 Enclave Boundary Defense  MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COEB-1 Enclave Boundary Defense  MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COED-2 Scheduled Exercises and Drills  MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COED-1 Scheduled Exercises and Drills  MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COEF-2 Identification of Essential Functions  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COEF-1 Identification of Essential Functions  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
COMS-2 Maintenance Support  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

Security Controls (Continuity)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
COMS-1 Maintenance Support MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COPS-3 Power Supply MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COPS-2 Power Supply MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COPS-1 Power Supply MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COSP-2 Spares and Parts MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COSP-1 Spares and Parts MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COSW-1 Backup Copies of Critical SW MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
COTR-1 Trusted Recovery MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

2. Security Design and Configuration Controls

Security Controls (Security Design and Configuration)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
DCAR-1 Procedural Review MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCAS-1 Acquisition Standards Confidentiality Level: Public, Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCBP-1 Best Security Practices MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCCB-2 Control Board MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCCB-1 Control Board MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCCS-2 Configuration Specifications MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCCS-1 Configuration Specifications MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCCT-1 Compliance Testing MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Security Design and Configuration)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
DCDS-1 Dedicated IA Services MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCFA-1 Functional Architecture for AIS Applications MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCHW-1 HW Baseline MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCID-1 Interconnection Documentation MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCII-1 IA Impact Assessment MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCIT-1 IA for IT Services MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCMC-1 Mobile Code MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCNR-1 Non-Repudiation MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Security Design and Configuration)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
DCPA-1 Partitioning the Application MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCPB-1 IA Program and Budget MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCPD-1 Public Domain Software Controls MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCPP-1 Ports, Protocols and Services MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCPR-1 CM Process MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCSD-1 IA Documentation MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCSL-1 System Library Management Controls MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCSP-1 Security Support Structure Partitioning MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
DCSQ-1 Software Quality	<input type="checkbox"/> YES <input type="checkbox"/> Inherited	<input type="checkbox"/> Risk Accepted	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times	0000/00/00

DoD Annual FISMA Guidance – FY08

MAC I, MAC II or MAC III	<input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Partial		<input type="checkbox"/> NO	0000/00/00
--------------------------	--	----------------------------------	--	-----------------------------	------------

DoD Annual FISMA Guidance – FY08

Security Controls (Security Design and Configuration)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
DCSR-3 Specified Robustness – High  Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
DCSR-2 Specified Robustness – Medium  Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
DCSR-1 Specified Robustness – Basic  Confidentiality Level: Public	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
DCSS-2 System State Changes  MAC I, MAC II or Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
DCSS-1 System State Changes  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
DCSW-1 SW Baseline  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

3. Enclave Boundary Defense Controls

Security Controls (Enclave Boundary Defense)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
EBBD-3 Boundary Defense Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBBD-2 Boundary Defense Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBBD-1 System State Changes Confidentiality Level: Public	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBCR-1 Connection Rules MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBPW-1 Public WAN Connection Confidentiality Level: Public or Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBRP-1 Remote Access for Privileged Functions Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBRU-1 Remote Access for User Functions Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
EBVC-1 VPN Controls MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

	<input type="checkbox"/> NA			
--	-----------------------------	--	--	--

4. Enclave and Computing Environment Controls

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECAD-1 Affiliation Display Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECAN-1 Access for Need-to-Know Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECAR-3 Audit Record Content Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECAR-2 Audit Record Content Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECAR-1 Audit Record Content Confidentiality Level: Public	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting MAC I , MAC II or; Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECAT-1 Audit Trail, Monitoring, Analysis and Reporting MAC III or;	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Confidentiality Level: Public or Sensitive					
--	--	--	--	--	--

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECCD-2 Changes to Data MAC I, MAC II or Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECCD-1 Changes to Data MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECCM-1 COMSEC Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECCR-3 Encryption for Confidentiality (Data at Rest) Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECCR-2 Encryption for Confidentiality (Data at Rest) Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECCR-1 Encryption for Confidentiality (Data at Rest) Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECCT-2 Encryption for Confidentiality (Data in Transit)  Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/000/0  0000/00/00
ECCT-1 Encryption for Confidentiality (Data in Transit)  Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECDC-1 Data Changes Controls  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECIC-1 Interconnections among DoD Systems and Enclaves  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECID-1 Host Based IDS  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECIM-1 Instant Messaging  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECLC-1 Audit of Security Label Changes  Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECLO-2 Logon Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECLO-1 Logon Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECLP-1 Least Privileges Confidentiality Level: Public, Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECML-1 Marking and Labeling Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECMT-2 Conformance Monitoring and Testing Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECMT-1 Conformance Monitoring and Testing Confidentiality Level: Public or Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECND-2 Network Device Controls MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECND-1 Network Device Controls MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECNK-2 Encryption for Need-To-Know Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECNK-1 Encryption for Need-To-Know Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECPA-1 Privileged Account Control MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECPC-2 Production Code Change Controls MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECPC-1 Production Code Change Controls MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
ECRC-1 Resource Control Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECRG-1 Audit Reduction and Report Generation  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECRR-1 Audit Record Retention  Confidentiality Level: Public, Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECSC-1 Security Configuration Compliance  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECSD-2 Software Development Change Controls  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECSD-1 Software Development Change Controls  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECTB-1 Audit Trail Backup  MAC I, MAC II or Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECTC-1 Tempest Controls  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Enclave and Computing Environment)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
ECTM-2 Transmission Integrity Controls  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECTM-1 Transmission Integrity Controls  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECTP-1 Audit Trail Protection  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECVI-1 Voice over IP  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECVP-1 Virus Protection  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECWM-1 Warning Message  Confidentiality Level: Public, Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
ECWN-1 Wireless Computing and Networking  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

5. Identification and Authentication Controls

Security Controls (Identification and Authentication)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
IAAC-1 Account Control  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IAGA-1 Group Identification and Authentication  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IAIA-2 Individual Identification and Authentication  Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IAIA-1 Individual Identification and Authentication  Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IAKM-3 Key Management  Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IAKM-2 Key Management MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IAKM-1 Key Management MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Identification and Authentication)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s)  YYYY/MM/DD
IATS-2 Token and Certificate Standards  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
IATS-1 Token and Certificate Standards  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

6. Physical and Environmental Controls

Security Controls (Physical and Environmental)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
PECF-2 Access to Computing Facilities Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PECF-1 Access to Computing Facilities Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PECS-2 Clearing and Sanitizing Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PECS-1 Clearing and Sanitizing Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEDD-1 Destruction Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEDI-1 Data Interception Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

Security Controls (Physical and Environmental)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
PEEL-2 Emergency Lighting MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEEL-1 Emergency Lighting MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEFD-2 Fire Detection MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEFD-1 Fire Detection MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEFI-1 Fire Inspection MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEFS-2 Fire Suppression System MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEFS-1 Fire Suppression System MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

Security Controls (Physical and Environmental)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
PEHC-2 Humidity Controls MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEHC-1 Humidity Controls MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEMS-1 Master Power Switch MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEPF-2 Physical Protection of Facilities Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEPF-1 Physical Protection of Facilities Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PEPS-1 Physical Security Testing Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PESL-1 Screen Lock MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

DoD Annual FISMA Guidance – FY08

Security Controls (Physical and Environmental)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
PESP-1 Workplace Security Procedures  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
PESS-1 Storage  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
PETC-2 Temperature Controls  MAC I or MAC II	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
PETC-1 Temperature Controls  MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
PETN-1 Environmental Control Training  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
PEVC-1 Visitor Control to Computing Facilities  Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
PEVR-1 Voltage Regulator  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

7. Personnel Controls

Security Controls (Personnel)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
PRAS-2 Access to Information Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PRAS-1 Access to Information Confidentiality Level: Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PRMP-2 Maintenance Personnel Confidentiality Level: Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PRMP-1 Maintenance Personnel Confidentiality Level: Pubic or Sensitive	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PRNK-1 Access to Need-to-Know Information Confidentiality Level: Public, Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PRRB-1 Security Rules of Behavior or Acceptable Use MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00
PRTN-1 Information Assurance Training Confidentiality Level: Sensitive or Classified	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00 0000/00/00

8. Vulnerability and Incident Management Controls

Security Controls (Vulnerability and Incident Management)	Control Implemented Correctly & Completely (Valid)	Risk Accepted or Control Not Fully Implemented	Weakness Listed on System POA&M	Control Tested Last 12 Months	Date of Last Test(s) YYYY/MM/DD
VIIR-2 Incident Response Planning  MAC I	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
VIIR-1 Incident Response Planning  MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00
VIVM-1 Vulnerability Management  MAC I, MAC II or MAC III	<input type="checkbox"/> YES <input type="checkbox"/> Inherited <input type="checkbox"/> NO <input type="checkbox"/> NA	<input type="checkbox"/> Risk Accepted <input type="checkbox"/> Partial	<input type="checkbox"/> POA&M <input type="checkbox"/> Mitigated	<input type="checkbox"/> 1 Time <input type="checkbox"/> 2+ Times <input type="checkbox"/> NO	0000/00/00  0000/00/00

(INTENTIONALLY BLANK)

## ATTACHMENT 5

### CONTINGENCY PLAN DEVELOPMENT AND TESTING GUIDANCE

1. PURPOSE. This attachment provides guidance on developing an IT Contingency Plan (CP) and includes a sample format that organizations can use as a template (Annex A). A CP is a crucial element when developing, using, or maintaining IT services, products, and support. This guidance is based on IT contingency planning best practices such as those provided in National Institute of Standards and Technology Special Publication (SP) 800-34 which may be consulted for more detailed guidance.

#### 2. DEVELOPING AN IT CONTINGENCY PLAN

##### a. Overview

(1) When developing a CP, there are three major areas to consider in the preparation to assure the plan will be effective during a disaster or other contingency situation. First, a Risk Management program will minimize the chances of many contingencies and help reduce the impact when one does occur. In addition, a risk assessment is used to identify the appropriate systems requiring a CP and to what extent they need coverage.

(2) Another area to consider is assuring the CP is addressed throughout a system's development life cycle. Although a CP is mainly related to the operational stage of a system, there are benefits in considering contingency preparation early in system development and acquisition, e.g., cost savings of including backup assets in initial system acquisitions.

(3) Finally, the relationship of the CP with other disaster or emergency plans needs to be considered. In DoD, the Continuity of Operations Plan (COOP) is the primary source to follow in order to keep the Component mission going. The CP can be considered one part of the COOP.

b. Contingency Planning and the Risk Management and Mitigation Process

(1) The Department of Defense manages risk to its information systems through the DIACAP. The risk management process considers the information system MAC and the confidentiality level of information handled (i.e., processed, stored, displayed or transmitted).

(a) The MAC and confidentiality levels reflected in DoDI 8500.2 are derived at the enterprise (DoD) level through consideration of potential threats, documented vulnerabilities, protection measures, and need-to-know.

(b) Risk management is conducted and integrated in the life cycle for an information system. There must be a specific schedule for periodically assessing and mitigating mission risks caused by major changes to the system and the processing environment due to changes resulting from policies and new technologies.

(2) Risk management encompasses a broad range of activities to identify, control, and mitigate risks to an information system. Risk management activities from the IT contingency planning perspective have two primary functions.

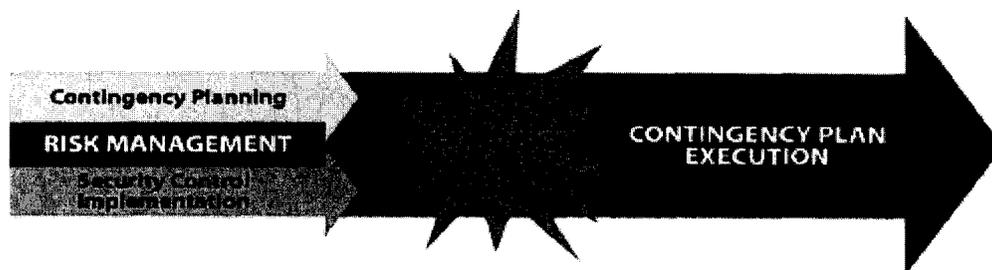
(a) First, risk management should identify threats and vulnerabilities so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. These security controls protect an information system against three classifications of threats.

1. Natural (e.g., hurricane, tornado, flood, and fire)

2. Human (e.g., operator error, sabotage, implant of malicious code, and terrorist attacks)

3. Environmental (e.g., equipment failure, software error, telecommunications network outage, and electric power failure.)

(b) Second, risk management must identify residual risks for which IT CPs must be put into place. Figure 1 below illustrates the relationship between identifying and implementing DoDI 8500.2 security controls, developing and maintaining the CP, and implementing the CP once the event has occurred.



**Figure 1. Contingency Planning as an Element of Risk Management Implementation**

c. Emergencies and IT Contingency Requirements

(1) IT CP and the COOP

(a) A COOP provides procedures and capabilities to sustain an organization's essential, strategic functions using alternate procedures. It addresses the subset of an organization's missions that are deemed most critical, is usually written at headquarters level, and not IT focused.

(b) An IT CP provides procedures and capabilities for recovering a major application (i.e., AIS) or enclave. It specifically addresses system disruptions and is not business process focused.

(2) The objectives of an IT CP include:

(a) Preparation for meeting the challenges of threats identified during the risk assessment.

(b) Ensuring the continuous performance of an organization's mission essential functions (MEFs)/operations during an emergency.

(c) Protecting mission essential equipment, records, and other assets.

(d) Reducing or mitigating disruptions to operations.

(e) Reducing damage and losses.

(f) Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

d. Contingency Capabilities

(1) Plans and procedures. An IT CP is developed and documented and, when implemented, provides for continued performance of essential information system functions under all circumstances. At a minimum, the plan:

- (a) Delineates MEFs and activities.
- (b) Outlines a decision process for determining appropriate actions in implementing IT CPs and procedures.
- (c) Establishes a roster of fully equipped and trained personnel with the authority to perform MEFs and activities.
- (d) Includes procedures for employee advisories, alerts, and IT CP activation, with instructions for relocation to pre-designated facilities, with and without warning, during duty and non-duty hours.
- (e) Provides for personnel accountability throughout the duration of the emergency.
- (f) Provides for attaining operational capability.
- (g) Establishes reliable processes and procedures to acquire resources necessary to continue MEFs and sustain operations.

(2) Identification of MEFs. Organization MEFs are the basis for IT contingency planning. In identifying MEFs, DoD organizations:

- (a) Identify all functions performed by the organization and then determine which should be continued under all circumstances.
- (b) Prioritize these MEFs.
- (c) Establish staffing and resources requirements needed to perform MEFs.
- (d) Identify mission critical data and systems necessary to conduct MEFs.

(e) Defer functions not deemed essential to immediate organizational needs until additional personnel and resources become available.

(f) Integrate supporting activities to ensure that MEFs can be performed as efficiently as possible during emergency relocation.

e. Plan Testing, Training, and Exercise

(1) Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element is tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas are addressed in a contingency test:

- (a) System recovery on an alternate platform from backup media.
- (b) Coordination among recovery teams.
- (c) Internal and external connectivity.
- (d) System performance using alternate equipment.
- (e) Restoration of normal operations.
- (f) Notification procedures.

(2) To derive the most value from the test, the organization develops a test plan designed to test the selected element(s) against explicit test objectives and success criteria. The use of test objectives and success criteria enables the effectiveness of each plan element and the overall plan to be assessed. The test plan may include a schedule detailing the time frames for each test and test participants. The test plan also delineates clear scope, scenario, and logistics. The scenario chosen may be a worst case incident or an incident most likely to occur. It also mimics reality as closely as possible.

(3) Current DoD guidance requires that contingency plan testing be conducted a minimum of once per year.

(4) The following list contains samples of the type of testing that may be conducted at the installation level:

(a) Classroom Exercises. Participants in classroom exercises, often called tabletop, walk through the procedures without any actual recovery operations occurring. Classroom exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise.

(b) Functional Exercises. Functional exercises are more extensive than tabletops, requiring the event to be faked. Functional exercises include simulations and wargaming. Often, scripts are written out for role players pretending to be external organization contacts, or there may be actual interagency and vendor participation. A functional exercise might include actual relocation to the alternate site and/or system cutover.

(5) Announcing the test in advance is a benefit to team members so that they can prepare for test mentally and have time to prioritize their workload. It is likely that some team members will not be available because of absence or because the test may be disruptive to their workload.

(a) Personnel availability issues are beneficial to the plan to capture how a real response may play out, thus providing critical input to plan modifications. It is important that an exercise must never disrupt normal operations. If testing at the alternate facility, the organization should coordinate test dates and operations with the facility.

(b) Test results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan.

(6) Alert and notification. A call tree activation scenario ensures that all personnel on the contingency response team or their alternate can be contacted. This test verifies telephone and cell phone numbers as well as the ability of each contingency team element to respond when primary members cannot be contacted. The test can terminate at any point desired. For example, only the call tree can be tested or all personnel can be called up and a table top training event conducted.

(7) Training for personnel with contingency plan responsibilities complements testing. Training is provided at least annually; new hires who will have plan responsibilities receive training shortly after they are hired. Ultimately, IT CP personnel are trained to the extent that they are able to execute their respective recovery procedures

without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Recovery personnel are trained on the following plan elements:

- (a) Purpose of the plan.
- (b) Cross-team coordination and communication.
- (c) Reporting procedures.
- (d) Security requirements.
- (e) Team-specific processes (notification/activation, recovery, and reconstitution phases).
- (f) Individual responsibilities (notification/activation, recovery, and reconstitution phases).

f. Type Accreditations and Inherited CP Controls

(1) All controls inherited from enclaves to which AIS applications are deployed are tested as part of an enclave's contingency exercise.

(2) For continuity controls, the program office must identify controls retained as a program office responsibility and those that are inherited from the enclaves to which the AIS application is deployed.

(a) The program office is responsible for developing a CP including security controls that remain a program office responsibility.

(b) The program office documents controls inherited from enclaves running the AIS application in its CP.

(3) Enclaves are responsible for maintaining and testing inherited IA controls without further guidance from the PM.

(a) The PM is responsible for preparing baseline control guidance when the AIS application is deployed.

(b) Any changes required in baseline controls will be disseminated to system operators for integration into the enclave CP.

g. Contingency Plan Maintenance

(1) Because the IT CP contains potentially sensitive operational and personnel information, its distribution is marked accordingly and controlled.

(2) Typically, copies of the plan are provided to recovery personnel for storage at home and office.

(3) A copy is also stored at the alternate site and with the backup media.

(4) The organization maintains a record of copies of the plan and to whom they were distributed.

ATTACHMENT 5, ANNEX A

SAMPLE IT CONTINGENCY PLAN (CP) FORMAT

SECTION I: INTRODUCTION

*(The Introduction section orients the reader to the type and location of information contained in the plan. Generally, the section includes the Purpose, Applicability, Scope, References/Requirements, and Record of Changes.)*

1.1 PURPOSE. *(This subsection establishes the reason for developing the IT CP and defines the plan objectives.)* This {system name} CP establishes procedures to recover the {system name} following a disruption. The following objectives have been established for this plan:

a. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

(1) Notification/Activation phase to detect and assess damage and to activate the plan.

(2) Recovery phase to restore temporary IT operations and recover damage done to the original system.

(3) Reconstitution phase to restore system processing capabilities to normal operations.

b. Identify the activities, resources, and procedures needed to carry out {system name} processing requirements during prolonged interruptions to normal operations.

c. Assign responsibilities to designated {Organization name} personnel and provides guidance for recovering {system name} during prolonged periods of interruption to normal operations.

d. Ensure coordination with other {Organization name} staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 **APPLICABILITY** *(The subsection documents the organization(s) impacted by the IT CP. All related plans that support or are supported by the IT CP should be identified and their relationship should be described. These related plans should be included as appendices to the CP.)*

a. The {system name} CP applies to the functions, operations, and resources necessary to restore and resume {Organization name}'s {system name} operations as it is installed at primary location name. The {system name} CP applies to {Organization name} and all other persons associated with {system name} as identified under Section 2.3, Responsibilities.

b. The {system name} CP is supported by plan name, which provides the purpose of plan. Procedures outlined in this plan are coordinated with and support the plan name, which provides purpose of plan.

1.3 **SCOPE** *(The scope discusses the issues, situations, and conditions addressed and not addressed in the plan. The section identifies the target system and the locations covered by the CP if the system is distributed among multiple locations.<sup>1</sup> The scope should address any assumptions made in the plan, such as the assumption that all key personnel would be available in an emergency. However, assumptions should not be used as a substitute for thorough planning.<sup>2</sup>)*

a. Planning Principles. Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles.

(1) The {Organization name}'s facility in (location), is inaccessible; therefore, {Organization name} is unable to perform {system name} processing for the DoD Component.

---

<sup>1</sup> For example, the plan may not address short-term disruptions expected to last fewer than four hours, or it may not address catastrophic events that result in the destruction of the IT facility.

<sup>2</sup> For example, the plan should not assume that disruptions would occur only during business hours; by developing a contingency plan based on such an assumption, the Contingency Planning Coordinator might be unable to recover the system effectively if a disruption were to occur during non-business hours.

(2) A valid agreement exists with the alternate site that designates that site in (location), as the {Organization name}'s alternate operating facility.

(a) {Organization name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency situation that prevents access to the original facility.

(b) The designated computer system at the alternate site has been configured to begin processing {system name} information.

(c) The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

b. Assumptions.

(1) Based on these principles, the following assumptions were used when developing the IT CP.

(a) The {system name} is inoperable at the {Organization name} computer center and cannot be recovered within 48 hours.

(b) Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.

(c) Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.

(d) Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.

(e) {system name} hardware and software at the {Organization name} original site are unavailable for at least 48 hours.

(f) Current backups of the application software and data are intact and available at the offsite storage facility.

(g) The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in City, State.

(h) Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

(2) The {system name} CP does not apply to the following situations:

- (a) Overall recovery and continuity of business operations.
- (b) Emergency evacuation of personnel.
- (c) Any additional constraints should be added to this list.

**1.4 REFERENCES/REQUIREMENTS** (*This subsection identifies the DoD requirement for contingency planning.*)

a. This {system name} CP complies with the {Organization name}’s IT contingency planning policy as follows:

The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

b. The {system name} CP also complies with the following federal and DoD policies:

- (1) The Computer Security Act of 1987
- (2) OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- (3) Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999
- (4) Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998

(5) PDD 63, Critical Infrastructure Protection, May 1998

(6) Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999

(7) Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000

(8) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," 6 February 2003.

(9) *Any other applicable DoD or DoD Component policies should be added.*



## SECTION 2. CONCEPT OF OPERATIONS

*(The Concept of Operations section provides additional details about the system, the contingency planning framework; and response, recovery, and resumption activities.)*

**2.1 SYSTEM DESCRIPTION AND ARCHITECTURE.** *(It is necessary to include a general description of the system covered in the CP. The description should include the IT system architecture, location(s), and any other important technical considerations.)* Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

**2.2 LINE OF SUCCESSION.** *(The order of succession identifies personnel responsible to assume authority for executing the CP in the event the designated person is unavailable or unable to do so.)*

The {organization name} sets forth an order of succession, in coordination with the order set forth by the department to ensure that decision-making authority for the {system name} CP is uninterrupted.

a. The Chief Information Officer (CIO), {organization name} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {system name} CP.

b. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority.

c. Continue description of succession as applicable.

**2.3 RESPONSIBILITIES.** *(The Responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation.)*<sup>3</sup>

---

<sup>3</sup> Teams and team members should be designated for specific response and recovery roles during contingency plan activation. Roles should be assigned to team positions rather than to a specific individual. Listing team members by role rather than by name not only reduces confusion if the member is unavailable to respond but also helps reduce the number of changes that would have to be made to the document because of personnel turnover.

a. The following teams have been developed and trained to respond to a contingency event affecting the IT system.

b. The CP establishes several teams assigned to participate in recovering {system name} operations.

(1) The {team name} is responsible for recovery of the {system name} computer environment and all applications. Members of the team name include personnel who are also responsible for the daily operations and maintenance of {system name}. The team leader title directs the {team name}.

*(Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation. Describe each team separately, highlighting overall recovery goals and specific responsibilities.)<sup>4</sup>*

c. The relationships of the team leaders involved in system recovery and their member teams are illustrated in Figure XX below.

(Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.)

---

<sup>4</sup> Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

### SECTION 3. NOTIFICATION AND ACTIVATION PHASE

*(This section defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. The notification and activation phase includes activities to notify recovery personnel, assess system damage, and implement the plan.)<sup>5</sup>*

3.1 This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {system name}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator (CPC).

In an emergency, the {Organization name}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

a. Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

(1) The first responder is to notify the CPC. All known information must be relayed to the CPC.

(2) The systems manager is to contact the Damage Assessment Team Leader and inform them of the event. The CPC is to instruct the Team Leader to begin assessment procedures.

(3) The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the Damage Assessment Team is to follow the outline below.

b. Damage Assessment Procedures: *(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)*

(1) Upon notification from the CPC, the Damage Assessment Team Leader is to ....

(2) The Damage Assessment Team is to ....

---

<sup>5</sup> At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.

c. Alternate Assessment Procedures:

(1) Upon notification from the CPC, the Damage Assessment Team Leader is to ....

(2) The Damage Assessment Team is to ....

(a) When damage assessment has been completed, the Damage Assessment Team Leader is to notify the CPC of the results.

(b) The CPC is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.

(c) Based on assessment results, the CPC is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

d. The CP is to be activated if one or more of the following criteria are met:

(1) {System name} will be unavailable for more than 48 hours.

(2) Facility is damaged and will be unavailable for more than 24 hours.

(3) Other criteria, as appropriate.

e. If the plan is to be activated, the CPC is to notify all Team Leaders and inform them of the details of the event and if relocation is required.

f. Upon notification, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

g. The CPC is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

h. The CPC is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the Organization's arrival.

i. The CPC is to notify remaining personnel (via notification procedures) on the general status of the incident.

## SECTION 4. RECOVERY OPERATIONS

*This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities. Recovery operations begin after the CP has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized.<sup>6</sup>*

4.1 The following procedures are for recovering the (system name) at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

### 4.2 RECOVERY GOALS (Objectives)

a. State the first recovery objective as determined by the Business Impact Assessment (RA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

(1) (team name)

– Example of Team Recovery Procedures

**Recovery Process for the LAN Recovery Team:**

*These procedures are used for recovering a file from backup tapes. The LAN Recovery Team is responsible for reloading all critical files necessary to continue production.*

- |  |              |
|--|--------------|
| • Identify file and date from which file is to be recovered  | Time: __: __ |
| • Identify tape number using tape log book   | Time: __: __ |
| • If tape is not in tape library, request tape from recovery facility; fill out with appropriate authorizing signature | Time: __: __ |
| • When tape is received, log date and time   | Time: __: __ |
| • Place tape into drive and begin recovery process   | Time: __: __ |
| • When file is recovered, notify LAN Recovery Team Leader  | Time: __: __ |

(2) (team name)

– Team Recovery Procedures

<sup>6</sup> Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site.

(3) (team name)

– Team Recovery Procedures

b. State the second recovery objective as determined. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

(1) (team name)<sup>7</sup>

– Team Recovery Procedures

(2) (team name)

– Team Recovery Procedures

(3) {team name}

– Team Recovery Procedures

c. State the remaining recovery objectives (as determined by the RA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

---

<sup>7</sup> Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.

## SECTION 5. RETURN TO NORMAL OPERATIONS

*This section discusses activities necessary for restoring {system name} operations at the {Organization name}'s original or new site. When the computer center at the original or new site has been restored, {system name} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.*

**5.1 ORIGINAL or NEW SITE RESTORATION.** Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- {team name}
  - Team Resumption Procedures
- {team name}
  - Team Resumption Procedures

**5.2 CONCURRENT PROCESSING.** Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- {team name}
  - Team Resumption Procedures
- {team name}
  - Team Resumption Procedures

**5.3 PLAN DEACTIVATION.** Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- {team name}
  - Team Testing Procedures

## SECTION 6. PLAN APPENDICES

The appendices included should be based on organizational, system, and plan requirements. Appendices to consider include:

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Continuity of Operations Plan.

(INTENTIONALLY BLANK)

ATTACHMENT 6

IA WORKFORCE AND TRAINING DATA COLLECTION INSTRUCTIONS

1. DOD SPECIFIC IA WORKFORCE FISMA METRIC TEMPLATES

a. This section captures detailed, training metric data relating to the IA workforce. Although the initial data call is due with the FY08 FISMA response on July 18, 2008, **Components will be permitted to provide updated IA training metrics until August 29, 2008.**

b. Note that Tables 1-4 in this attachment are for illustrative purposes only and the actual data will be entered in the corresponding spreadsheets in Attachment 9. The completed data from IA Workforce spreadsheets will automatically populate the aggregate cells of the separate spreadsheet for OMB Template, Section B, Question 6. Each DoD Component must respond to the training metrics and provide a short narrative describing the training provided (Question 6.c).

c. DoD employees with access to IT systems are required to receive initial IA awareness training prior to being granted access to the system(s) and annual IA awareness training to retain access according to Department of Defense Directive (DoDD) 8570.1. DoD Components must document and maintain the status of awareness training for each user. DoD 8570.01-M establishes minimum baseline IA awareness training requirements.

(1) Pursuant to ASD(NII)/DoD CIO Memorandum, "DoD Information Assurance Awareness Training Requirement," dated August 27, 2007, the DoD is designated as a Shared Service Center (SSC) for IA Awareness training under the OMB Information System Security Line of Business (ISS LoB) initiative. The DoD SSC is the provider of the "DoD IA Awareness" training course to meet the requirements of DoD 8570.01-M. This course is developed by the Defense Information Systems Agency (DISA) on behalf of the DoD SSC.

(2) Effective August 27, 2007, DoD Components were to stop funding development of in-house IA materials that duplicated "DoD IA Awareness" content. However, the DoD Components are still responsible for funding their unique requirements.

(3) As of October 2007, all DoD Components are required to use the DoD SSC as their IA Awareness provider. The "DoD IA Awareness" course is used to meet the FISMA mandated annual DoD awareness requirement.

d. Employees with significant IA responsibilities perform functions defined in DoD 8570.01-M on a full-time, part-time, or embedded duty status. These functions may be performed by military, government civilians, or contractors performing IA management or technical roles for a DoD information system.

e. Per ASD(NII)/DoD CIO Memorandum, "Use of Peer-to-Peer (P2P) File-Sharing Applications across DoD," dated November 23, 2004, P2P file-sharing is an information technology that permits computer users to share files with other users without centralized security controls or oversight. DoD Components are encouraged to identify and eliminate unauthorized P2P file-sharing activities originating in or traversing their networks. As part of this effort, IA awareness training addresses unauthorized P2P file-sharing on DoD systems. DoD Components shall comply with this guidance.

## 2. IA WORKFORCE QUANTITATIVE DATA REPORTING REQUIREMENTS

a. IA workforce positions and manning status. Identify all positions per Chapters 3-5 of DoD 8570.01-M, required to execute IA functions as primary or additional/ embedded duties. Note that starting in 2009, Components will also be required to separately identify positions for Information Assurance System Architecture and Engineering (IASAE) and Computer Network Defense Service Provider (CNDSP) as detailed in Change 1 of DoD 8570.01-M.

(1) Any position/person required to perform IA functions included in the DoD 8570.01-M Chapters 3-5 are considered significant and must be reported as part of the IA workforce regardless of whether they are performed as primary or additional/embedded duties. However, no position/person should be counted more than once. If someone is performing multiple IA functions use the one they spend the highest percent of time/effort performing.

(2) Enter primary duty IA positions in Table 1.

(3) Enter Additional/embedded duty IA positions in Table 2.

(4) Additional positions/personnel performing specialized IA functions include Information Assurance System Architect and Engineer (IASAE), and Computer Network Defense Service Provider (CND SP). If these duties are performed as a subset of the

Information Assurance Technical (IAT) or Information Assurance Management (IAM) functions defined in DoD 8570.01-M, use those categories and levels.

(5) Enter the number of IAT and IAM positions filled, by category and level, in Tables 1 and 2.

(6) Enter the number of IAT and IAM positions filled with “trained” incumbents by category and level in Tables 1 and 2.

(7) Enter the number of IAT and IAM positions filled with “certified” incumbents by category and level in Tables 1 and 2 (“certified” individuals are a subset of “trained” individuals).

<b>Table 1. IA Workforce Primary Duty Positions</b>											
	<b>Civilian</b>				<b>Military</b>				<b>*Contractor</b>		
	Positions	Filled	Trained	Certified	Positions	Filled	Trained	Certified	Filled	Trained	Certified
<b>IAT I</b>											
<b>IAT II</b>											
<b>IAT III</b>											
<b>IAM I</b>											
<b>IAM II</b>											
<b>IAM III</b>											
<b>DAA</b>											
<b>Total</b>											
<b>*Contractors do not have positions</b>											

*Note: Starting in 2009, Components will also be required to separately identify Information Assurance System Architecture and Engineering (IASAE) and Computer Network Defense Service Provider (CNDSP) positions. These templates are images of the Excel spreadsheets that are provided separately with this guidance and data should be entered and saved for reporting to DoD in the Excel spreadsheets.*

**Table 2. IA Workforce Additional/Embedded Duty Positions**

	Civilian			Military				*Contractor			
	Positions	Filled	Trained	Certified	Positions	Filled	Trained	Certified	Filled	Trained	Certified
<b>IAT I</b>											
<b>IAT II</b>											
<b>IAT III</b>											
<b>IAM I</b>											
<b>IAM II</b>											
<b>IAM III</b>											
<b>DAA</b>											
<b>Total</b>											
*Contractors do not have positions											

*Note: IA positions are any that require performance of any functions by category and level per the DoD 8570.01-M. Do not double count individuals performing functions in multiple IA categories.*

b. Enter the number of users with DoD information system access (“Required”) versus the number who completed DoD IA Awareness training requirements (“Completed”) in Table 3. Of the “Completed” total, enter into the “DoD SSC” column the number which met the requirement by taking the “DoD IA Awareness” training course developed by the DoD SSC.

**Table 3. IA User Training**

<b>Required</b>	<b>Completed</b>	<b>DoD SSC</b>

c. Enter the total dollars obligated or expended for IA training and certification in Table 4.

<b>Table 4. IA Workforce (WF) Training and Certification Milestone Budget Plan *</b>							
<b>IA WF Budget</b>	<b>(FY07)</b>	<b>(FY08)</b>	<b>(FY09)</b>	<b>(FY10)</b>	<b>(FY11)</b>	<b>(FY12)</b>	<b>Total</b>
<b>Required</b>							
<b>Budgeted</b>							
<b>Obligated</b>							
* Identify data to the extent available for FY08-FY12.							

### 3. IA WORKFORCE DEFINITIONS

a. **Categories, Levels, and Functions.** The structure for identifying all DoD Information Assurance (IA) positions and personnel.

(1) Categories. The DoD IA workforce is split into major categories of Technical and Management. Management refers to personnel performing any IAM functions described in Chapters 4 or 5 of DoD 8570.01-M

(2) Levels. Each of the IA workforce categories has levels (Technical or Management Level I, II, and III). The management category also includes the DAA as defined in DoD 8570.01-M.

(3) Functions. High level tasks required to successfully perform IA category for an information system. The function indicates the tasks that an employee performs or occupational requirements to successfully perform as part of the IA Workforce. For the purposes of the DoD IA workforce functions have been associated with a category and level. These functions provide a means to distinguish between different levels of work. The functional level approach also encourages a broader, more integrated means of identifying what an employee must know to perform the tasks that comprise an IA position across all of the DoD Components.

**b. Duty Positions (Tables 1 & 2).** Applies to both positions and individuals (as identified in DoD 8570.01-M).

(1) **Primary.** An IA position with primary duties focused on IA functions. The position may have other duties assigned, but the main effort focuses on IA functions. The position would normally require at least 25 to 40(+) hours per week devoted to IA functions (see Table 1).

(2) **Additional.** A position requiring a significant portion of the incumbent's attention and energies to be focused on IA functions, but in which IA functions are not their primary responsibilities. The position would normally require 15 to 24 hours, out of a 40(+) hour week, devoted to IA functions (see Table 2).

(3) **Embedded.** A position with IA functions identified as an integral part of other major assigned duties. These positions normally require up to 14 hours, out of a 40(+) hour week be devoted to IA related functions (see Table 2).

**c. Information Assurance Management (IAM) Levels.** These may be known as Information Assurance Officers, System Security Officers, Information System Security Managers, Information Assurance Officers, etc (as identified in DoD 8570.01-M).

(1) **IAM Level I.** IAM Level I personnel are responsible for the implementation and operation of a DoD IS or system component within their Computing Environment (CE). Incumbents ensure that IA related IS are functional and secure within the CE. Applies knowledge of IA policy, procedures, and structure to develop, implement, and maintain a secure CE. Chapter 4 Table C4.T3. of DoD 8570.01-M contains a complete list of functions for IAM-I.

(2) **IAM Level II.** IAM Level II personnel are responsible for the IA program of an IS within the Network Environment (NE). Incumbents in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure that IS are functional and secure within the NE. Applies knowledge of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure NE. IAM Level II position functions are listed in Table C4.T5 of DoD 8570.01-M.

(3) **IAM Level III.** IAM Level III personnel are responsible for ensuring that all enclaves IS are functional and secure. They determine the enclaves' long term IA systems needs and acquisition requirements to accomplish operational objectives. They also develop and implement information security standards and procedures through the DoD certification and accreditation process. Applies knowledge of IA policy,

procedures, and workforce structure to develop, implement, and maintain a secure enclave environment. IAM Level III position functions are listed in Table C4.T7 in DoD 8570.01-M.

(4) DAA. The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority defined by the Committee on National Security Systems Instruction No. 4009 (reference (r)). See Chapter 5 of DoD 8570.01-M.

**d. Information Assurance Technical (IAT) Levels.** These may also be named system administrators, help desk, security administrators, etc.

(1) IAT Level I. IAT Level I personnel make the CE less vulnerable by correcting flaws and implementing IAT controls in the hardware or software installed within their operational systems. Chapter 3 Table C3.T3. of DoD 8570.01-M contains a complete list of functions for IAT-I.

(2) IAT Level II. IAT Level II personnel provide NE and advanced level CE support. They pay special attention to intrusion detection, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are well secured. These positions focus on threats and vulnerabilities and improve the security of systems. IAT Level II personnel have mastery of the functional requirements of the IAT Level I position. Chapter 3 Table C3.T5. of DoD 8570.01-M contains a complete list of functions for IAT-II.

(3) IAT Level III. IAT Level III personnel focus on the enclave environment and support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the CE, NE, and enclave environments. They apply extensive knowledge of a variety of the IA field's concepts, practices, and procedures to ensure the secure integration and operation of all enclave systems. IAT Level III personnel have mastery of the functional requirements of both the IAT Level I and Level II positions. IAT Level III position functions are listed in Table C3.T6 of DoD 8570.01-M.

**e. Local National Employee.** Civilians or contractors, whether paid from appropriated or non-appropriated funds, employed or used by the U.S. Forces in a foreign country who are nationals or non-U.S. residents of that country.

**f. Positions.** For the sole purpose of FISMA reporting, IA positions are described as specific billets in a unit's table of organization (T/O) or manning document which are occupied by individuals with IA responsibilities, regardless of actual job series

classification or whether IA responsibilities represent a primary or secondary job responsibility. Under the DoD 8570.01-M, any position requiring the performance of information system management or privileged access IA functions as identified in Chapters 3, 4, and 5 of the Manual, must be identified as part of the IA workforce. This requirement applies to military and civilian positions including those staffed by local nationals (LN).

**g. IAT and IAM Category Training Requirements.** Note training must be aligned to the IA functional requirements of the position. Participation in initial training (classroom, distributive, or blended) before, or immediately on, assignment of IA responsibilities is mandatory. Training need not result in award of a military specialty code (e.g., Military Occupational Specialty, Navy Enlisted Classification Code, and/or Air Force Specialty Code), but must be aligned to the IA functions required of the position.

(1) Training Definitions.

(a) **Resident.** Instructor led classroom instruction based on specific performance criteria.

(b) **Distributive.** Computer based training (CBT) via website, computer disc, or other electronic media.

(c) **On the job training (OJT).** Supervised hands on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.

(d) **Blended.** A combination of instructor led classroom training and distributed media. This may also include instructor led classroom training using distributed multi-media.

(2) Certification Definition. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval, based on a set of standards for a specific profession or occupation's functional job levels. Each certification is designed to stand on its own, and represents an individual's mastery of a particular set of knowledge and skills.

(INTENTIONALLY BLANK)

ATTACHMENT 7

IT SECURITY POA&M REPORTING GUIDANCE

1. **PURPOSE.** The primary purpose of an IT Security Plan Of Action and Milestones (POA&M) is to assist agencies in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities.

a. OMB requires agencies to prepare IT Security POA&Ms for all programs and systems in which an IT security weakness has been found. OMB guidance directs CIOs and the DoD Component program officials to develop, implement, and manage IT Security POA&Ms for all programs and systems they operate and control (for program officials this includes all systems that support their operations and assets, including those operated by contractors).

b. In addition, program officials are required to update the agency CIO on their progress on at least a quarterly basis and at the direction of the CIO. This enables the CIO to monitor agency-wide remediation efforts and provide the agency’s quarterly update to OMB.

2. **TYPES.** There are three types of IT Security POA&Ms, as reflected in Table 1 below. Examples of Component and System level POA&M Templates are provided in Figures 1 and 2. For an in-depth discussion of the POA&M process and instructions for completing each type of POA&M, refer to the DIACAP, DoDI 8510.01.

Type of IT Security POA&M	Responsibility	Submit To	Dates Due
System-level	PMs/IAMs	DoD Component CIO  (Also to DoD SIAO for systems with a CAT I weakness or on the OMB Watch List (Exhibit 300) for security)	1 Dec, 1 Mar, 1 Jun, 1 Sep
DoD Component-level	DoD Component CIO	ASD(NII)/DoD CIO	Due with the annual FISMA report and as directed
DoD Enterprise	ASD(NII)/DoD CIO	OMB	As directed

**Table 1. Three Types of IT Security POA&Ms**

System Level IT Security POA&M Example											
<b>Date Initiated:</b>	October 1, 2005			<b>IS Type:</b>	Enclave			<b>OMB Project #:</b>	009-202334-55174		
<b>Date Last Updated:</b>	January 15, 2006			<b>(See Note 1)</b>				<b>(See Note 2)</b>			
<b>Component Name:</b>	OSD			<b>POC Name:</b>	James Avery						
<b>System / Project Name:</b>	DoD Network			<b>POC Phone:</b>	703-698-7733			<b>Security Costs:</b>	(\$62,500)		
<b>DoD IT Registration No.:</b>	14753			<b>POC E-Mail:</b>	james.avery@osd.mil						
Weakness (1) (See Note 4)	CAT (2)	IAAC and Impact Code (3)	POC (4)	Resources Required (5)	Scheduled Completion Date (6)	Milestones with Completion Dates (7)	Milestone Changes (8)	Source Identifying Weakness (9)	Status (10)	Comments (11)	
1 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 - 2/15/2005; 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 12/10/15/2005 due to inadequate funding	\$500.0 IA Controls Test Conducted 5/15/2005	Ongoing	Funding will be available in FY 2006	
2 Security plan is out of date, more than one year since last update despite new interconnections	II	DCSD-2 Impact High	IAO	\$5,000	11/30/2005	Update plan and obtain independent review - 11/30/2005		\$500.0 IA Controls Test Conducted 5/15/2005	Ongoing		
3 Lack of accurate systems hardware and software baseline hampers implementation of Configuration Management processes.	II	DCSEW-1 DCSW-1 Impact High	IAO	\$0	8/31/2005	Establish baseline inventory of the hardware and software and utilize revision control system - 5/15/2005. Implement software revision control program - 2/31/2005		Security Test and Evaluation - 4/15/2005	Completed - 10/30/2005		
4 Encryption is not certified FIPS 140-2 compliant.	III	DCOE-1 Impact Medium	IAO	\$5,000	10/20/2005	Upgrade encryption software to FIPS 140-2 certified version 10/20/2005		IS Audit 3/21/2005	Ongoing	May slip due to delay in funding	
5											
6											
7											
8											
9											
10											
11											

Figure 1. System-level IT Security POA&M Example

Component Level IT Security POA&M Example							
Date:	March 1, 2005	POC Name:	Mr. Navy CIO				
Component Name:	DON	POC Phone:	555-555-5555				
		POC E-mail:	dncio@nav.mil				
Weakness (1)	POC (2)	Resources Required (3)	Scheduled Completion Date (4)	Milestones with Completion Dates (5)	Milestone Changes (6)	Source Identifying Weakness (7)	Status (8)
1 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
2 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
3 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		Naval Audit Service	Ongoing

Figure 2. Component-level IT Security POA&M Example

(INTENTIONALLY BLANK)

## ATTACHMENT 8

### DEFINITIONS

**Continuity of Operations Plan (COOP) (DoDD 3020.26).** Documented procedures for an internal effort within individual components of the Executive, Legislative, and Judicial Branches of Government assuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies. COOP involves plans and capabilities covering the same functional objectives of Continuity of Government (COG), must be maintained at a high level of readiness, and be capable of implementation both with and without warning. COOP is not only an integral part of COG and Enduring Constitutional Government (ECG), but is simply "good business practice" - part of the Department of Defense's fundamental mission as a responsible and reliable public institution.

**Designated Accrediting Authority (DAA) (DoDI 8510.01).** The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (DoDI 8500.2 leads with the term designated approving authority, which was favored at the time of publication)

**DoD Components (DoDD 8500.01E).** The office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department.

**DoD Information System (DoDD 8500.01E).** Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

**IT Contingency Plan (CP) (NIST SP 800-34).** Documented procedures for interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

**Material Weakness (OMB Circular No. A-123).** A material weakness in internal control is a reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. Material weaknesses in internal control over financial reporting shall be included in the annual Federal Managers Financial Integrity Act (FMFIA) report, but separately identified. A significant deficiency (see below) under FISMA is to be reported as a material weakness under the FMFIA.

**National Security System (44 USC, Sec 3542).** Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency – (i) the function, operation, or use of which involves intelligence activities; involves crypto logic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

**Privileged User (DoDI 8500.2).** An authorized user who has access to system control, monitoring, or administration functions.

**Significant Deficiency (OMB FY04 FISMA Guidance).** A weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers' Financial Integrity Act (FMFIA).

(INTENTIONALLY BLANK)

ATTACHMENT 9

OMB-DoD TEMPLATES

*The OMB electronic file templates, with DoD-specific spreadsheet additions, will be provided separately e-mailed in electronic form to your FISMA Point of Contact as a Microsoft Excel file. All responses must be recorded and returned in this workbook file.*