



**DEPARTMENT OF THE NAVY**  
BUREAU OF MEDICINE AND SURGERY  
2300 E STREET NW  
WASHINGTON DC 20372-5300

IN REPLY REFER TO  
6000  
Ser M6/10UM6164  
24 Sep 10

MEMORANDUM FOR COMMANDER, NAVY MEDICINE EAST  
COMMANDER, NAVY MEDICINE WEST  
COMMANDER, NAVY MEDICINE NATIONAL CAPITAL AREA  
COMMANDER, NAVY MEDICINE SUPPORT COMMAND

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

Ref: (a) through (o) (See enclosure (1))

Encl: (1) References  
(2) Navy Medicine Enterprise Information Assurance (EIA) Web-based System Checklist  
(3) Navy Medicine Enterprise Information Assurance (EIA) Controlled Unclassified Checklist

1. Purpose

a. This policy establishes Information Assurance (IA) requirements for non-traditional information technology systems, such as web-based systems, which are not hosted within the Navy Medicine accreditation boundaries. Non-traditional systems provide services to the Navy Medicine Enterprise without deploying major system components in the traditional sense. This policy does not change Department of Defense (DoD) or Department of Navy (DON) policy concerning operation and security of the Navy Medicine Information Enterprise, including the Global Information Grid (GIG), nor does it alter in any way the Navy Medicine Governance processes for Information Management (IM)/Information Technology (IT) investments.

b. This policy defines five categories of web-based systems, a set of requirements to provide adequate security for Navy Medicine Controlled Unclassified Information (CUI) on these categories of web-based systems, and an evaluation process to identify the appropriate category for a given web-based system. Each category dictates what level of review is required by Navy Medicine stakeholders. All new web-based systems, regardless of category, must be evaluated and approved per this policy prior to being used operationally in the Navy Medicine environment. This policy also defines corresponding roles and responsibilities and refers to but does not define Navy Medicine Governance processes.

2. Background

a. Per reference (a), DoD-owned Information Systems (ISs) and DoD-controlled ISs operated by a contractor or other entity on behalf of the DoD that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, are subject to the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) to ensure appropriate protection of DoD information and ISs. The decision whether to process a system for a full Navy Accreditation effort is predominantly based on the traditional view of a system (i.e., system components located within the Navy Medicine accreditation boundary). Yet, many healthcare capabilities are outsourced, which involve connections to non-DoD systems and services (e.g., secure-messaging).

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

Web-based systems used to support these capabilities may require processing of CUI, including Personally Identifiable Information (PII), Protected Health Information (PHI), information marked For Official Use Only (FOUO), and other Sensitive Information.

b. The level of protection afforded Navy Medicine information is dependent upon three factors: sensitivity of the information, responsibility for the IS, and responsibility for the network on which the IS resides. Information that is considered “Sensitive” requires protection greater than information suitable for public release, per references (b) through (d). Sensitive Information is an example of CUI, which includes, but is not limited to, information identified/labeled as PII, PHI, and FOUO. Responsibility for the IS and whether it resides on Navy Medicine site networks or within their accreditation boundary impacts the process by which the system is reviewed and permitted to process Navy Medicine CUI. Under the process defined below, the network (or enclave) on which the IS resides will determine whether the DON DIACAP process is required. A web-based system, for example, may reside and function entirely outside the Navy Medicine network, hence may not be subject to the full DON DIACAP process.

c. Once the three factors in paragraph 2b are clearly identified, the appropriate requirement(s) and level of effort to provide the minimum necessary security to Navy Medicine information can be determined. Effective IA relies on a combination of these requirements, which are listed below.

(1) DIACAP: full C&A per DON DIACAP process. Note: DIACAP requires that a Privacy Impact Assessment (PIA) is completed for an IS that is used to collect, maintain, or disseminate PII.

(2) PPS/UTNPP: verification of DoD Ports, Protocols, Services (PPS) Category Assurance List (CAL) and Navy Unclassified Trusted Network Protect Policy (UTNPP), per reference (e).

(3) PIA: assessment of the IT system to determine whether PII in electronic form is collected, maintained or disseminated in a manner that protects the privacy of individuals. The PIA also documents the requirement for a System of Records Notice (SORN), the IT system’s security, and departmental compliance.

(4) Support Agreement: used to document details of the service provided, including all parties to the agreement, applicable statutory authority, purpose and scope of services to be provided, responsibilities, resource commitments, liability, ownership, legal/financial considerations, effective period, and PII/PHI requirements, where applicable.

(5) Directive-Type Memoranda (DTM) 08-027: this policy requires a contract, grant, or other legal agreement that documents IA requirements in addition to what is required of a Support Agreement to ensure adequate security for all Navy Medicine CUI specifically on non-DoD ISs.

(6) IA Assessment: assessment of risks to Navy Medicine information and information systems to determine necessary process for assuring appropriate security and privacy controls. IA assessment is also embedded in DIACAP.

d. Figure 1 below depicts the requirements above in a tree diagram, grouped into three main decision points: information sensitivity (is it CUI?), network (is it a Navy Medicine network?), and information system (is it a DoD system?). The boxes to the right indicate the requirements/process required for each branch end point.

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

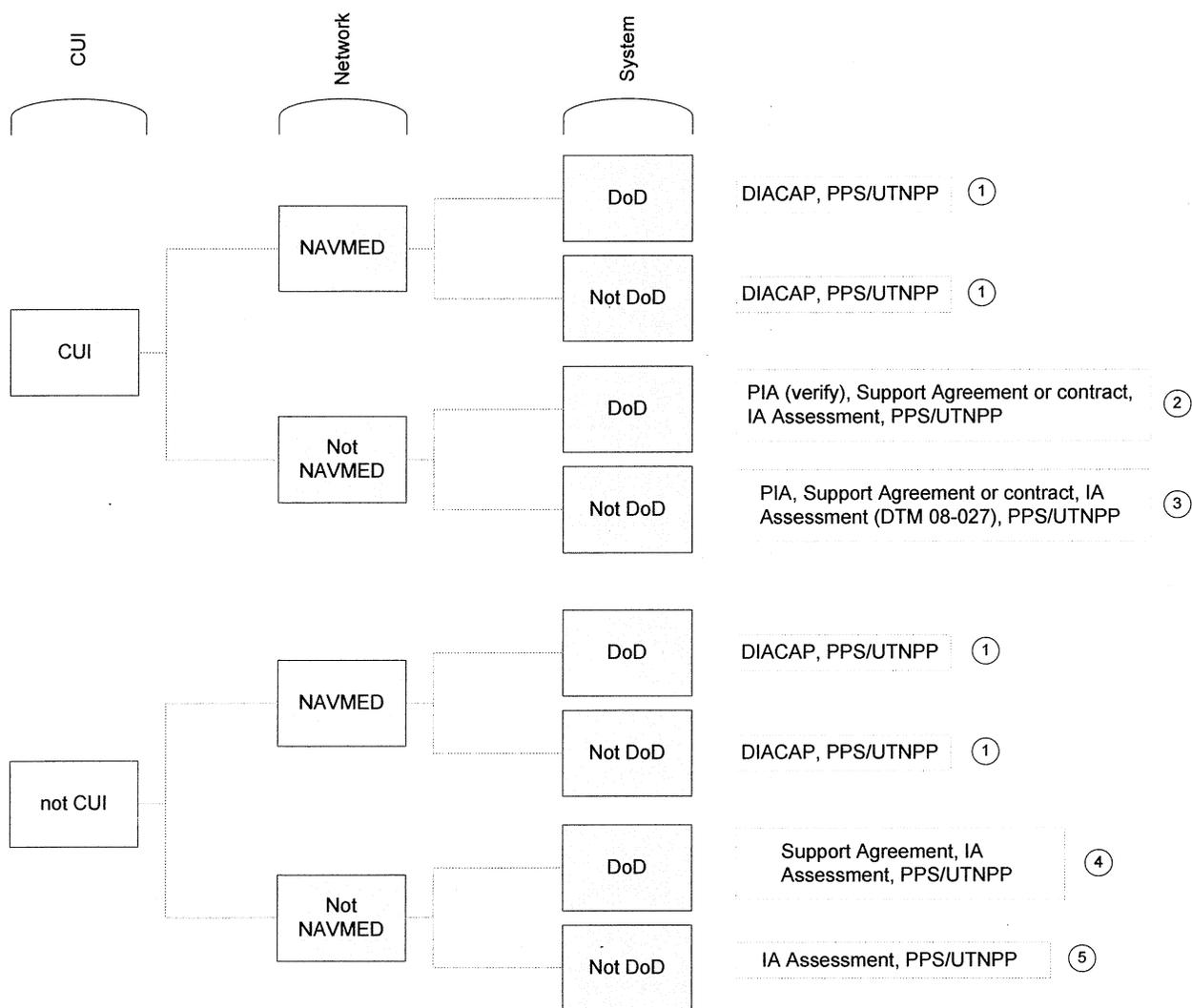


Figure 1: IA requirements decision tree, grouped into five categories (depicted by circled numbers to the right)

From the IA requirements decision tree above, there are five unique categories of IA requirements based on the information/network/IS combinations.

(1) Category 1: Navy Medicine user(s) connected outbound, inbound, or bi-directionally to DoD or internet/commercial based system with or without the exchange of Navy Medicine CUI. Some or all of the system resources are hosted within the Navy Medicine site accreditation boundary (e.g., TRICARE Management Activity/Military Health System Program of Record, commercial system hosted (partially or entirely) in Navy Medicine environment).

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

(2) Category 2: Navy Medicine user(s) connected outbound to a DoD system with the exchange of Navy Medicine CUI. No system components are hosted on Navy Medicine assets and/or within the Navy Medicine accreditation boundary (e.g., non-Navy DoD hospitals where patient data is being exchanged).

(3) Category 3: Navy Medicine user(s) connected outbound to internet/commercial based system with the exchange of Navy Medicine CUI. No systems components are hosted on Navy Medicine assets and/or within the Navy Medicine accreditation boundary (this is synonymous with Category 2, though the system is not hosted within the DoD, e.g. commercial partners and hospitals where patient data is being exchanged).

(4) Category 4: Navy Medicine user(s) connected outbound to DoD system with no exchange of Navy Medicine CUI. No system components are hosted on Navy Medicine assets and/or within the Navy Medicine accreditation boundary (e.g., Defense Knowledge Online (DKO), milSuite, TroopTube, etc.).

(5) Category 5: Navy Medicine user(s) connected outbound to internet/commercial based system with no exchange of Navy Medicine CUI. No system components are hosted on Navy Medicine assets and/or within the Navy Medicine accreditation boundary (this is synonymous with Category 4, though the system is not hosted within the DoD, e.g., Google, library/research portal, etc.).

3. Policy. It is BUMED policy to ensure the appropriate protection of Navy Medicine information, ISs, and networks. BUMED encourages the use of approved commercial systems to support the healthcare mission.

a. Approval to use any web-based system that is used to collect, maintain, or disseminate CUI, including PII, must minimally meet the requirements set forth in this policy. The duration of approval will not exceed 3 years from the date signed or the period of performance of the contract, grant, or other legal agreement, as stipulated in paragraph 3.b.

b. Per reference (f), it is DoD policy to provide adequate security for all unclassified DoD information on non-DoD information systems. Appropriate requirements, including but not limited to information safeguards, shall be incorporated into all contracts, grants, and other legal agreements or understandings with non-DoD entities.

c. Per reference (g), all services provided to BUMED activities which are outside the scope of the BUMED Supplier's current BUMED Instruction (BUMEDINST) 5450 Mission and Functions Statement must be documented by a support agreement, regardless of whether reimbursement is required.

d. Per reference (h), DON activities are required to perform a PIA on any IT system that collects PII on members of the public and DON civilian and military personnel.

e. Per reference (i), it is DoD policy that PIAs are completed on DoD ISs and electronic collections that collect, maintain, use, or disseminate PII, including those ISs and electronic collections supported through contracts with external sources.

f. Per reference (f), (h), and (i), all non-DoD ISs that collect, maintain, use, or disseminate Navy Medicine PII require a DON PIA.

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

g. Per reference (a) and (j), all DoD-owned ISs and DoD-controlled ISs operated by a contractor or other entity on behalf of the DoD that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, are required to obtain authorization to operate via the DIACAP process. All DIACAP packages require completion of a PIA for ISs that collect, maintain, or disseminate PII.

h. Per reference (k) through (m), sensitive information transmitted via E-Mail shall be encrypted. This applies to PHI and PII.

i. Per reference (f), the loss or unauthorized disclosure of PII (including PHI) must be reported in compliance with DoD 5400.11-R and other DoD information safeguarding policies, and implemented by the insertion of applicable requirements into contracts, grants, and other legal agreements or understandings. Reference (n) summarizes DON and DoD PII incident reporting requirements.

4. Responsibilities. Timely and effective IA assessments require support from leadership, IA stakeholders, functional managers, and resource and operation managers. The following responsibilities are assigned to ensure a well-managed, repeatable IA assessment process for web-based systems within the Navy Medicine enterprise.

a. Program Manager. A web-based system to be considered for use in Navy Medicine is championed by a Program Manager (PM). The PM responsibilities described below only apply to IA requirements reflected in Categories 2, 3, 4, and 5.

(1) Ensure completion of all IA/privacy assessments, as appropriate.

(2) Complete a PIA, where applicable, with coordination from BUMED-M62.

(3) Coordinate completion and/or verification of all contracts, grants, or other legal agreements with appropriate BUMED stakeholders, as required.

(4) Sign and present to BUMED-M62 an assessment that contains the results and recommendations of all security and privacy assessments, and assurance that appropriate security and privacy requirements are included in a contract, grant, or other legal agreement. The assessment will include the results of all actions corresponding to the identified category of web-based system as well as a cover letter. The assessment must contain the necessary information by which BUMED-M6 can review and approve the web-based system presented.

b. Navy Medicine Information Systems Support Activity (NAVMISSA) Enterprise IA (EIA). Web-based systems are reviewed by the NAVMISSA EIA team to determine the appropriate IA “path” for ensuring protection of Navy Medicine information and information systems. Enclosures (2) and (3) are used to assess the disposition of the web-based system and protection of CUI processed/stored therein. All results are provided to the respective PM.

(1) Determine the appropriate category for each web-based system. This represents the initial decision point for determining the level and type of IA/privacy assessment and subsequent actions.

(2) Verify DoD PPS CAL and Navy UTNPP Compliance. *All Categories*

(3) Complete the CUI checklist. *All Categories*

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

(4) Coordinate completion and submission of a DIACAP package if the system resides (in part or entirely) on the Navy Medicine network, regardless of information sensitivity. This action results in an accreditation for the web-based system. *Category 1*

(5) Assess whether the IA requirements per references (f) and (k) are met in the ongoing deployment and/or life cycle management activities of the web-based system to protect Navy Medicine information and information systems. *Categories 2, 3, 4, 5*

(6) Forward to the PM the results of all IA assessments and actions, indicating whether the web-based system provides adequate security of Navy Medicine information. *Categories 2, 3, 4, 5*

c. BUMED-M62. Maintains liaison with the NAVMISSA EIA team, the PM, and the Governance team to ensure all IA/privacy issues are communicated and coordinated.

(1) Work with respective PMs to ensure that a PIA is completed for all web-based systems that collect, maintain, or disseminate PII. *Categories 2, 3*

(2) Review the assessment provided by the PM; verify completeness and accuracy. *Categories 2, 3, 4, 5*

(3) Create a formal designation package based on the PM-provided assessment; forward to BUMED-M6 for action. *Categories 2, 3, 4, 5*

(4) Inform stakeholders of BUMED-M6 web-based system designation (i.e., approval or non-approval for use). *Categories 2, 3, 4, 5*

d. BUMED-M6. Approving authority for all web-based systems that do not fall in Category 1. The Navy Operational Designated Approval Authority (ODAA) delegates authority in writing to the BUMED-M6 military or civilian staff member that satisfies DON qualifications. Applies to *Categories 2, 3, 4, 5*.

(1) Review BUMED-M62 designation package for web-based systems.

(2) For web-based systems approved for use, approve corresponding designation package.

(3) Submit quarterly reports to Navy ODAA on the status of category 2-5 web-based systems that were approved during the previous quarter that are subject to the provisions of this policy.

5. Process. Figure 2 below depicts the flow of responsibilities, actions, and deliverables from paragraph 4.

Subj: INFORMATION ASSURANCE REQUIREMENTS FOR WEB-BASED SYSTEMS  
SUPPORTING NAVY MEDICINE

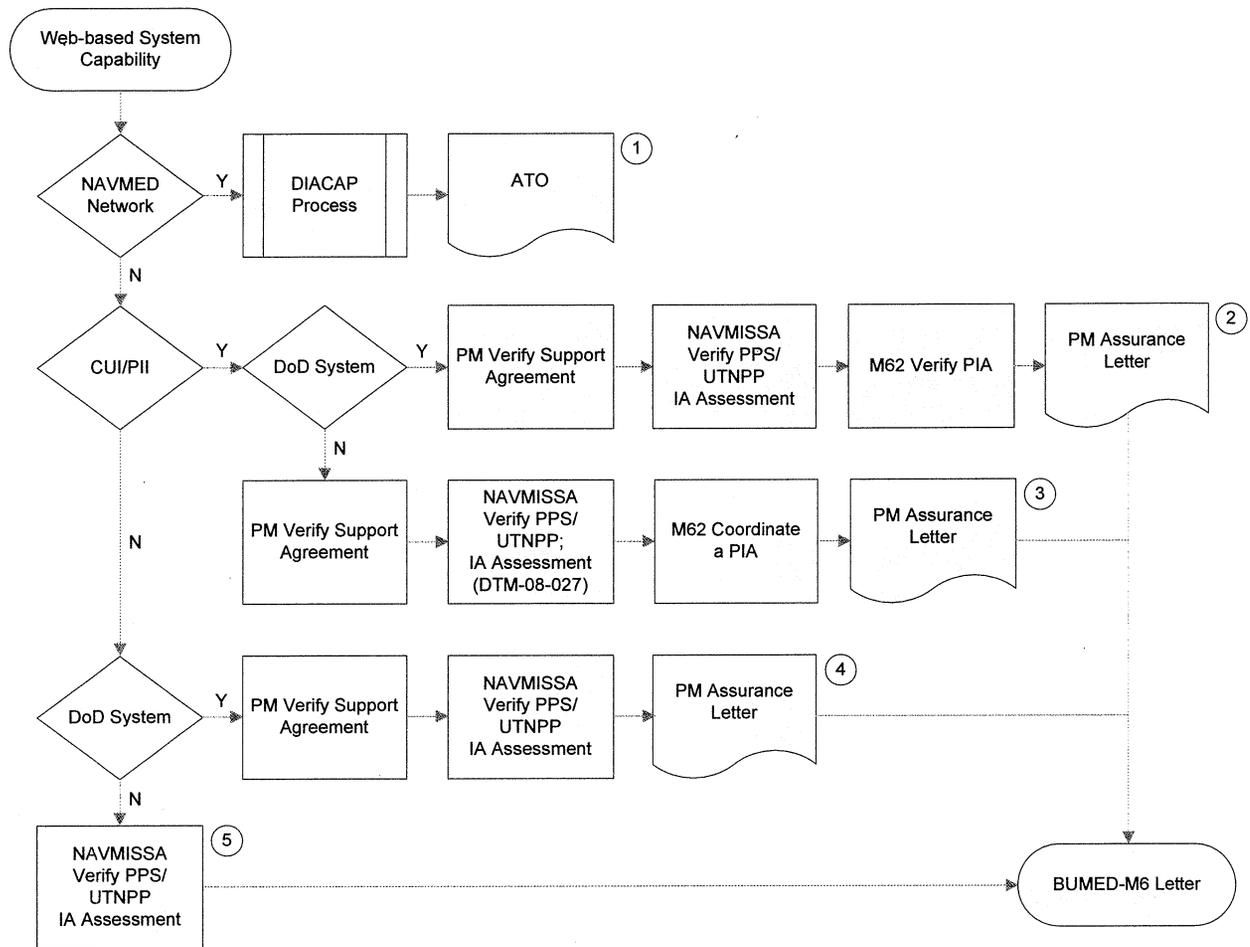


Figure 2: Actions & deliverables for web-based systems, mapped to five Categories

6. Contact. The point of contact for this matter is Mr. Verlin Hardin, at (202) 762-3180 or by e-mail: Verlin.Hardin@med.navy.mil.

7. Reports. The reporting requirements contained in this instruction are exempt from reports controlled per Part IV, paragraph 7k of reference (o).

*A. M. Robinson, Jr.*  
A. M. ROBINSON, JR.

## REFERENCES

- Ref:
- (a) DoDI 8510.01 of 28 Nov 2007, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
  - (b) DoD 8580.02-R of Jul 2007, Department of Defense Health Information Security Regulation
  - (c) SECNAVINST 5211.5E
  - (d) SECNAV M-5510.36 of June 2006, Department of the Navy Information Security Program
  - (e) CNO WASHINGTON DC 261722Z NOV 02, Promulgation of Navy-Marine Corps Unclassified Trusted Network (UTNPROTECT) Policy (NOTAL)
  - (f) ASD (NII)/DoD CIO DTM-08-027 of 31 Jul 2009, Security of Unclassified DoD Information on Non-DoD Information Systems
  - (g) BUMEDINST 7050.1A
  - (h) DON CIO WASHINGTON DC 181430Z MAY 09, Department of the Navy Privacy Impact Assessment Guidance
  - (i) DoDI 5400.16 of 12 Feb 2009, Department of Defense Privacy Impact Assessment Guidance
  - (j) Department of the Navy DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook of 15 July 08
  - (k) DoDI 8500.2 of 6 Feb 2003, Information Assurance (IA) Implementation
  - (l) DON CIO WASHINGTON DC 032009Z OCT 08, DON Policy Updates for Personal Electronic Devices (PED) Security and Application of E-Mail Signature and Encryption
  - (m) BUMED Memo 6000 Ser M09BK/07UMBK143 of 28 Jan 2008 (NAVMED Policy 08-005)
  - (n) BUMED Memo 5239 Ser M09B6/09UM09B6121 of 6 Jul 2009 (NAVMED Policy 09-016)
  - (o) SECNAVINST M-5214.1 of Dec 2005, Department of the Navy Information Requirements (Reports) Manual

NAVY MEDICINE ENTERPRISE INFORMATION ASSURANCE (EIA) WEB-BASED  
SYSTEM CHECKLIST

System Name: \_\_\_\_\_ Date: \_\_\_\_\_

Site Point of Contact: \_\_\_\_\_ EIA Rep: \_\_\_\_\_

1. Is the system, or parts of the system, hosted on Navy Medicine Assets or within Navy Medicine Accreditation boundaries?

a. If no, continue to question 2.

b. If yes, stop, submission of the full Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) package to the Operational Designated Approval Authority (ODAA) is required.

2. Does the system process Sensitive Information (Health Insurance Portability and Accountability Act (HIPAA), social security number (SSN), personally identifiable information (PII), For Official Use Only, etc.)?

a. If no, does the system use authorized Ports, Protocols, Services (PPS) as defined in the Department of Defense PPS Category Assurance List (CAL) and the Unclassified Trusted network Protection Policy (UTNPP)?

(1) If no, review of PPS options required. Exceptions will not normally be requested from Naval Network Warfare Command (NETWARCOM) PPS Management (PPSM) or Department of Defense PPSM; however, options such as business-to-business gateway or requesting vendor/host change ports may be a considered. Additionally, recommendations to the requestor on details of what other sites use may provide a compliant solution.

(2) If yes, is the internet protocol (IP) address of the connection on the Navy Cyber Defense Operations Command (NDOC) block list?

(a) If no, review complete. Please send review to Navy Medicine Information Systems Support Activity (NAVMISSA) Chain of command.

(b) If yes, verify with NCDOC the validity of block and if unable to resolve, deny request.

b. If yes, does the host site protect the data per the minimum standards detailed in DODI 8500.2 and DTM 08-027? (Use enclosure 3, Navy Medicine Enterprise Information Assurance Controlled Unclassified Information Checklist)

(1) If no, deny request for use of system.

(2) If yes, is the protection of sensitive information detailed in the contract or agreements (for commercial sites) or memorandum of agreement, memorandum of understanding, or Service certification and accreditation documentation (for Department of Defense systems)?

(a) If no, request host, vendor provide such documentation. If they will not, deny request for use of system

(b) If yes, go to the next, recommend approval of system and submit to NAVMISSA Program Office for approval.

Comments:

NAVMISSA EIA Reviewer

Signature/Date: \_\_\_\_\_

NAVY MEDICINE ENTERPRISE INFORMATION ASSURANCE (EIA) CONTROLLED  
UNCLASSIFIED INFORMATION CHECKLIST

System Name: \_\_\_\_\_ Date: \_\_\_\_\_

Site POC: \_\_\_\_\_ EIA Rep: \_\_\_\_\_

Per Directive Type Memorandum 08-027, the following are required for the protection of controlled unclassified information (CUI). Contracts and agreements shall address how applicable information safeguards will be implemented and cover all of the below.

Have the following requirements been addressed:

1. Do not process Department of Defense (DoD) information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.
2. Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
3. Sanitize media (e.g., overwrite) before external release or disposal.
4. Encrypt all information that has been identified as CUI when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best available encryption technology.
5. Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.
6. Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.
7. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.
8. Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web

site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

9. Provide protection against computer network intrusions and data exfiltration, minimally including the following:

a. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

b. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

c. Prompt application of security-relevant software patches, service packs, and hot fixes.

10. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled) as specified in contracts, grants, and other agreements.

11. Report loss or unauthorized disclosure of information per contract or agreement requirements and mechanisms.

12. All contracts and/or agreements will address how applicable information safeguards will be implemented?

13. Are all requirements in DODI 8500.2 for processing sensitive information met?

Are requirements 1-13 met? YES NO

Comments:

---

Navy Medicine Information Systems Support Activity EIA Reviewer Signature/Date