

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

**Unit Inspected:** \_\_\_\_\_ **Date:** \_\_\_\_\_

### Incident Handling and Reporting

Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
1. Does the organization have an incident response plan which identifies the responsible CND provider, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team?	AR 25-2, Para. 4-21c; DoDI 8500.2 IA Control VIIR	Review the organization's incident response plan and supporting documentation (appointment orders, training certificates, etc). Tenant organizations should have a copy of the service provider's incident response plan.		
2. Is the incident response plan reviewed/updated at least annually (or every six months for MAC-I systems)?	AR 25-2, Para. 4-21b; DoDI 8500.2 IA Control VIIR	Look for documentation (after action reports, memorandums for record, change log, etc.) showing that the incident response procedures were reviewed/updated and tested.		
3. Are users aware of their responsibility to cease all activity on a computer when they observe suspected security incidents or suspicious IS operation and report immediately to the System Administrator (SA), Information Assurance Manager (IAM), or the Information Assurance Security Officer (IASO)?	AR 25-2, Para. 3-3c(9), 4-22a through c	Interview users to determine how they would respond to an incident and who they would report it to.		
4. Does the incident response plan define conditions which require the generation of a Serious Incident Report (SIR)?	AR 25-2, Para. 4-21d; DoDI 8500.2 IA Control VIIR	Verify that the organization's incident response plan that defines the conditions for a SIR.		
5. Do IA personnel report information system security incidents on an ongoing basis?	AR 25-2, Para. 3-2d(3), f(13), and 3-3a(14)	Request copies of incident reports from IA personnel. Reports can be in the form of e-mail traffic, memorandums, trouble tickets, or other form of logging.		
6. Does the incident response plan include procedures to isolate the compromised system and preserve forensic evidence and chain of custody?	AR 25-2, Para. 4-22c and d; DoDI 8500.2 IA Control VIIR	1. Review the organization's incident response plan.  2. Survey users, SAs, IASOs, and the IAM to find out what actions they take on a compromised system.		
7. Is the organization aware of actions required prior to placing a compromised system back on the network?	AR 25-2, Para. 4-23a	Query the SA/IASO/IAM to determine if they know the proper actions to take prior to placing a compromised system back on the network.		
8. Does the organization understand the requirement to report and respond to classified information spillage events?	AR 25-2, Para. 4-21c(8) and d(3); BBP 03-VI-O-0001 (Classified Information Spillage), Para. 11	1. Survey users and interview incident response personnel.  2. View trouble tickets or incident reports and after action reports of when classified spillage procedures were practiced and view lessons learned.  3. Review the incident response plan for a section on handling classified information spillage incidents.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>IA Training and Certification</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
9. Does the command's IA user awareness training program comply with the Army minimum training requirements?	AR 25-2, Para. 4-3a(8); DoD 8570.01-M, Para. C6.1.6 and C6.2.5; DoDI 8500.2 IA Control PRTN	1. The requirement for initial/annual training must be documented in an SOP/IA policy.  2. Organization must ensure that the Information Assurance Awareness training is taken at the Fort Gordon IA site as a part of their training SOP/IA policy. However, the organization may provide additional IA awareness training tailored to their organization's mission. URL: <a href="https://ia.gordon.army.mil/dodiaa/default.asp">https://ia.gordon.army.mil/dodiaa/default.asp</a>		
10. Do all users complete IA Awareness training before receiving network access, and have they received awareness training within the past year?	AR 25-2, Para. 4-3a(8)(a and b), NIST 800-53 Appendix F AT2, CJCSM 6510.01 Appendix B Enclosure A Para. 5 and Appendix A Enclosure A Para. 7b, DoD 8570.01-M Para. C6.2.2; DODD 8570.1 5.9.2; DoDI 8500.2 IA Control PRTN	Review ATCTS. If some users are not in ATCTS, request documentation for the IA awareness training (initial/annual) and the AUP. Review the completion date on the training certificate.		
11. Have all IA personnel in Technical Levels I-III completed the required minimum training within six months of appointment to the position?	AR 25-2, Para. 4-3a(2), (6)(a-c) and 2-8; DoD 8570.01-M, Para: C3.2.3.1; IA Training and Certification Best Business Practice, Para. 11f, g, and h; DoDI 8500.2 IA Control PRTN, ATCTS CIO/G6 memorandum dated 7 Aug 07	Review ATCTS:  1. Verify all IA Technical personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Technical Level.  2. Review required minimum training and ensure all courses are completed or will be completed within 6 months of appointment.  3. Request copies of Privileged Access Agreements if not found in ATCTS.		
12. Have all IA personnel in Management Levels I-III completed the required minimum training within six months of appointment?	AR 25-2 Para. 4-3a(1),(3), (6) and 2-8; DoD 8570.01-M, Par C.4.2.3.6; Army IA Training and Certification Best Business Practice, Para. 11a ,b, and c	Review ATCTS:  1. Verify all IA Management personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Management Level.  2. Review required minimum training and ensure all courses are completed or will be completed within 6 months of appointment.  3. If applicable, request copies of Privileged Access Agreements.		
13. Have all IA personnel in Computer Network Defense-Service Provider Levels completed the required minimum training within six months of appointment to the position?	AR 25-2 Para. 4-3a; DoD 8570.01-M,Chapter 11; Army IA Training and Certification Best Business Practice, Para. 7	Review ATCTS:  1. Verify all IA Management personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Management Level.  2. Review IA Management personnel records to ensure organization is meeting the current certification milestone and have a plan to meet future milestones and reach 100%.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>IA Training and Certification</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
<p>14. Have all IA personnel in Information Assurance Security Architecture and Engineering Levels completed the required minimum training within six months of appointment to the position?</p> <p><b>TACTICAL SYSTEMS ONLY</b></p>	DoD 8570.01-M, Chapter 10; Army IA Training and Certification Best Business Practice, Para.9	<p>Review ATCTS:</p> <ol style="list-style-type: none"> <li>1. Verify all IASAE personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Management Level.</li> <li>2. Review required minimum training and ensure all courses are completed or will be completed within 6 months of appointment.</li> <li>3. If applicable, request copies of Privileged Access Agreements.</li> </ol>		
<p>15. Have all Designated Approving Authorities (DAA) completed the DAA Basics training upon appointment?</p> <p><b>TACTICAL SYSTEMS ONLY</b></p>	AR-2 Para 3-3m(1)(d)(e), 5-5g,h,k; DoD 8570.01-M, Par C5.1.1; IA Training and Certification Best Business Practice Para. 7d	<p>Review ATCTS:</p> <ol style="list-style-type: none"> <li>1. Verify that all DAA s have a profile in ATCTS to include a copy of the CIO/G6 appointment email (digitally signed).</li> <li>2. Review required minimum training and ensure the DAA Basic course was completed upon appointment. URL: <a href="https://ia.training.us.army.mil">https://ia.training.us.army.mil</a>.</li> <li>3. Review management training completions if applicabile.</li> </ol>		
<p>16. Have all Designated Approving Authorities (DAA) completed the DoD DAA computer-based training (CBT) or Web-based training (WBT) product within 60 days of assignment to the position?</p> <p><b>TACTICAL SYSTEMS ONLY</b></p>	AR-2 Para 3-3m(1)(d); DoD 8570.01-M, Par C5.3.1.1; IA Training and Certification Best Business Practice Par. 7d	<p>Review ATCTS:</p> <ol style="list-style-type: none"> <li>1. Verify that all DAA s have a profile in ATCTS to include a copy of the DAA training certificate.</li> <li>2. Review required training and ensure the DAA CBT/WBT course was completed within 60 days of appointment. URL: <a href="http://iase.disa.mil/eta/etadaa.html">http://iase.disa.mil/eta/etadaa.html</a></li> <li>3. Substitute training includes the National Defense University/Information Resource Management College, Information System Certification and Accreditation course (catalog #6209) and CNSSI 4012</li> </ol>		
<p>17. Have all IA personnel in Management Levels I-III obtained a DoD baseline commercial certification six months of appointment (new hires or reassignments after 19 Dec 2005); and has the organization met the appropriate certification milestone?</p>	AR 25-2, Para. 4-3a(1)(d); DoD 8570.01-M C4.2.3.2, C9.3.2.5 C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Table 1	<p>Review ATCTS:</p> <ol style="list-style-type: none"> <li>1. Verify all IA Management personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Management Level.</li> <li>2. Review IA Management personnel records to ensure organization is meeting the current certification milestone and have a plan to meet future milestones and reach 100%.</li> </ol>		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

<b>IA Training and Certification</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
18. Have all IA personnel in Technical Levels I-III obtained a DoD baseline commercial certification within six months of appointment (new hires or reassignments after 19 Dec 2005); and has the organization met the appropriate certification milestone?	AR 25-2 4.3a(6)(a)&(d); DoD 8570.1-M C3.2.4.1.1, C9.3.2.5, C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Table 1	Review ATCTS:  1. Verify all IA Technical personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Technical Level.  2. Review IA Technical personnel records to ensure organization is meeting the current certification milestone and have a plan to meet future milestones and reach 100%.		
19. Have all IA personnel in Computer Network Defense- Service Provider Levels obtained a DoD baseline commercial certification and Computing Environment (if applicable) within six months of appointment (new hires or reassignments after 16 May 2008); and has the organization met the appropriate certification milestone?  <b>TACTICAL SYSTEMS ONLY</b>	DoD 8570.1-M C11.2.4.1.2, C11.2.4.1.2, C11.2.4.7.2; IA Training and Certification BBP, Table 1	Review ATCTS:  1. Verify all IA CND-SP personnel have a profile in ATCTS to include appointment orders and assignment to appropriate CND-SP Level and Technical Level if applicable.  2. Review CND-SP personnel records to ensure organization is meeting the current certification milestone and have a plan to meet future milestones and reach 100%.		
20. Have all IA personnel in Information Assurance Security Architect and Engineer Levels obtained a DoD baseline commercial certification and Technical Level certification (if applicable) within six months of appointment (new hires or reassignments after 16 May 2008); and has the organization met the appropriate certification milestone?  <b>TACTICAL SYSTEMS ONLY</b>	DoD 8570.1-M C10.2.3.1.2, C10.2.3.2, C10.2.3.2.1; IA Training and Certification BBP, Table 1	Review ATCTS:  1. Verify all IA IASAE personnel have a profile in ATCTS to include appointment orders and assignment to appropriate IA Technical Level.  2. Review IASAE personnel records to ensure organization is meeting the current certification milestone and have a plan to meet future milestones and reach 100%.		
21. Do all contracts that include IA services specify the contractor certification and training requirements and are all IA function requirements to be performed by contractors included in their statement of work/contract including Local Nationals?	DOD 8570.1-M Par. C1.4.4.12, C7.3.4.4, C1.4.4.5, C2.1.5, C1.4.4.12, C3.2.4.8.1, C4.2.3.1	Review appropriate contract documentation (e.g. Statements of Work, Security Classification Guides) for compliance with this requirement doing the annual review and note this requirement on new contracts completed after 19 Dec 05.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>IA Vulnerability Management</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
22. Are Information Assurance Vulnerability Management (IAVM) messages acknowledged no later than the "Acknowledge by" date as stated in the IAV message?	AR 25-2, Para. 4-25a; DoDI 8500.2 IA Control VIVM	Review the A&VTR database to see when the IAVM messages were released and when the unit acknowledged receipt of them.		
23. Are IAVM corrective actions implemented within the listed suspense date on the IA Vulnerability Alert (IAVA)?	AR 25-2, Para. 4-24c(2); DoDI 8500.2 IA Control VIVM	1. A full IAVM vulnerability scan on all assets must be conducted.  2. Scan results must be reviewed to verify whether the patches have been applied to the vulnerable assets.		
24. Is IAVM compliance status reported in A&VTR or by manual submission in accordance with the IA Vulnerability Alert (IAVA)?	AR 25-2, Para. 4-25d	Review the A&VTR database or manual submission to ensure that the unit has reported IAVM compliance for each IAVM message within the required suspense date.		
25. If Plan of Actions and Milestones (POA&Ms) are required, are they being submitted and approved before the suspense date in A&VTR (or manual procedures)?	AR 25-2, Para. 4-25c and 4-27	1. Review the A&VTR database for POA&M submissions.  a. Ensure sufficient mitigating actions have been included and the Designated Approving Authority (DAA) has entered comments.  b. The local DAA can approve POA&Ms for up to 30 days.  c. For POA&Ms exceeding 30 days, waivers must be processed through RCIO and approved by HQDA.		
26. Are OU administrators (Sys Admins / IMOs / IAMs) conducting monthly IAVA compliance scans of all systems or reviewing weekly DOIM scan results?	Network Assessment Scanning BBP, Para. 12A(5); DoDI 8500.2 IA Control VIVM	Review previous scan results (past 90-180 days) to determine if monthly IAVA compliance scans are being conducted.		
27. Are all IA personnel subscribed to the Army Knowledge Online (AKO) IAVM Community Group Listserver?	AR 25-2, Para. 4-24 c(1)d	Have IA personnel show you the IAVM messages they received via email from the listserv. This includes all IA personnel (Sys Admins, IASOs, IAMs, OU Admins).		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>IA Program Management</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
28. Are personnel required to sign the appropriate AUP (privileged access and user access) prior to being granted access to the information system?	AR 25-2, Para. 3-3c(1), 4-3, and Appendix B; ALARACT 158-2008, Section 2; BBP 06-PR-M-0003 (Privileged Access Agreement AUP), Para. 8; BBP 06-EC-O-0008 (Data at Rest), Para. 8E; DoDI 8500.2 IA Control PRRB and PRTN	<ol style="list-style-type: none"> <li>1. Review a copy of each AUP (privileged access and user access) for appropriate content.</li> <li>2. Select a sample of privileged and nonprivileged users from Active Directory and request copies of the AUPs. Review in ATCTS.</li> </ol>		
29. Are procedures in place for clearing, purging, destroying and releasing unclassified systems memory, media, and devices to include records maintenance?	AR 25-2 Para. 4-18a through i; BBP Reuse of Computer Hard Drives, 17 Aug 06; DoDI 8500.2 IA Control PECS	<ol style="list-style-type: none"> <li>1. Examine the organization's procedures.</li> <li>2. Check with the responsible individual (ie. a DOIM or property book officer) to validate procedures for media turn-in and disposal are implemented.</li> <li>3. Review records of destruction on file.</li> </ol>		
30. Do authorized users who are contractors, DOD direct or indirect hires, foreign nationals, or foreign representatives have their respective affiliations displayed as part of their e-mail addresses?	AR 25-2 Para. 4-15a and 4-20f(8); DODI 8500.2 IA Control ECAD	Review the Global Address List for compliance with displaying the appropriate affiliation.		
31. Does management ensure that users understand that they have no expectation of privacy by enforcing the display of the Notice and Consent Banner every time a user logs on to an Army system?	AR 25-2 Para. 4-5m(3); ALARACT 158/2008, Para. 6 and 7; DoDI 8500.2 IA Control ECWM	<ol style="list-style-type: none"> <li>1. Survey users and ask if they understand that they have no expectation of privacy.</li> <li>2. Review the Notice and Consent Banner of the surveyed user's workstation to ensure users must take a positive action to accept the terms of the notice and consent banner before access is granted.</li> </ol>		
32. Do users meet the personnel security requirements for gaining access to Army information systems?	AR 25-2 Para. 4-5c(3) and 4-14a; DoDI 8500.2 IA Control PRAS	<ol style="list-style-type: none"> <li>1. Review access request form template (DD Form 2875) and completed forms on file.</li> <li>2. Interview selected organizational personnel with personnel security responsibilities (IAM, G-2/S-2, Security Manager).</li> <li>3. Interview supervisors to verify that they approve access and verify "need to know" of their employees.</li> </ol>		
33. Has the organization appointed IA personnel as required?	AR 25-2 Para. 2-24f; DoDI 8500.2 IA Control DCSD	Examine the organization's appointment orders for IA personnel.		
34. Are contractor personnel positions designated as IT-I, IT-II, IT-III, or IT-IV for access to the IS, have they satisfied the appropriate background check requirements, and are these requirements included in maintenance contracts, statements of work, and specified on the DD Form 254 (Department of Defense Contract Security Classification Specification)?	AR 25-2, Para. 4-14a; DoDI 8500.2 IA Control PRAS-1 (Sensitive) or PRAS-2 (Classified)	<ol style="list-style-type: none"> <li>1. Review the Statement of Work and the DD Form 254 for the type of work to be performed and the IT level required.</li> <li>2. Review appointment orders, if applicable, of contractor personnel assigned to IA roles.</li> <li>3. Verify that contractor employees' background investigations are initiated or periodic reinvestigations (PR), if required, have been submitted.</li> </ol>		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

<b>IA Program Management</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
35. Are foreign exchange personnel and representatives of foreign nations limited to email only access unless further access is authorized by the CIO/G-6?	AR 25-2 Para. 4-15b and 4-15d; DoDD 8500.01E Para. 4.9	1. Identify any foreign officials and review which user security groups they belong to. 2. Review waiver packets, if any.		
36. Does the organization submit MS4X and MX5T funding requirements?	AR 25-2, Para. 4-2 a and b; DoDI 8500.2 IA Control DCPB	Review the organization's MS4X (IA) and MX5T (COMSEC) requests and requirements in the ISSP database ( <a href="https://issp.army.mil">https://issp.army.mil</a> )		
37. Does the organization restrict the use of employee owned information systems (EOIS)?	AR 25-2, Para. 4-31; AR 25-1, Para. 6-1f(5)i	1. Ask and/or physically inspect to determine if any EOIS exist within the environment. If so, request approval documentation and review the organization's EOIS AUP. 2. Scan to determine if EOIS are present in an area.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Public Key Infrastructure</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
38. Are all CAC holder user accounts in Active Directory provisioned to use CAC Cryptographic Logon?	Army CIO/G-6 ALARACT Army Accelerated Implementation Of Common Access Card Cryptographic Network Logon, Para. 5.A; JTF-GNO Communications Task Order 06-02, Para. 5; AR 25-2, Para. 4-5c(6) and Para. 4-12a; DoDI 8500.2 IA Control IAIA and IAKM	1. Ask System Administrators to logon to the Active Directory accounts administration tool and verify that user accounts have a unique EDI-PI 10-digit number associated with each account.  2. Perform AD query for disabled smart card login settings on any accounts.		
39. Are all System Administrators using an Alternate Smart Card Logon (ASCL) Token to access their higher privileged account?	Army CIO/G-6 Memorandum, Subject: Alternative Smart Card Logon (ASCL) Token for Two-Factor Authentication, Para. 2 and 3; DoDI 8500.2 IA Control ECLP and IAKM	1. Ask System Administrators to logon with their ASCL Token.  a. Confirm that the logon window requires a PIN instead of a username and password.  b. Ask System Administrators to remove ASCL Token.  c. Confirm a message similar to this is displayed, "This computer has been locked. Only NNNNNNNNN@mil (Last Name, First Name) or an administrator can unlock this computer.		
40. Are Active Directory accounts for users with a CAC, Personal Identity Validation (PIV) compliant hardware token, or ASCL token configured for user-based enforcement?	JTF-GNO CTO 07-015, Public Key Infrastructure (PKI) Implementation, Phase 2, Task 2; Army PKI Phase 2 Implementation Instructions, Version 2.2, Para. 5.2 (Task 2)	1. Ask System Administrators to logon to the Active Directory accounts administration tool and verify that user accounts have a unique EDI-PI 10-digit number associated with each account.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Certification and Accreditation</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
41. Does the organization have a copy of an approved Network Change Proposal (NCP) / Tenant Security Plan (TSP) and a current Authority to Connect (ATC) and is the NCP/TSP being maintained?	AR 25-2, Para. 5-10(a); DoDI 8510.01 DIACAP	<p>1. Review approval documents in 8th US Army portal and ensure organization has a copy. Ensure ATC memo has not expired.</p> <p>2. Ensure the organization is maintaining their Network Change Proposal (NCP) with any changes (e.g., hardware/software updates, IA personnel appointment orders, network topology diagrams, system updates, etc.) within the past 30 days.</p> <p>3. Verify the organization has not changed the security configuration of their network(s) without submitting a new NCP/TSP IAW current ATC.</p>		
42. Has a System Owner (SO) been identified for each sponsored PEO/PM information system or locally-developed information system?	DoDI 8510.01 DIACAP	Check the C&A tracking matrix, located at IACORA home on the AKO at <a href="https://www.us.army.mil/suite/page/146650">https://www.us.army.mil/suite/page/146650</a> , for SO information. The spreadsheet is sortable by system name or SO name.		
43. Does the sponsored PEO/PM information system or locally-developed information system have a current Interim Authorization To Test (IATT), Interim Approval To Operate (IATO) or Approval To Operate (ATO)?	AR 25-2, Para. 5-8(b); Army Information Assurance Certification and Accreditation BBP, Para. 10.L; DoDI 8510.01, E3. Enclosure 3, The DIACAP Package	<p>1. Check the C&amp;A tracking matrix, located at IACORA home on the AKO at <a href="https://www.us.army.mil/suite/page/146650">https://www.us.army.mil/suite/page/146650</a>, for approval expiration date. The spreadsheet is sortable by system name or Accreditation Termination Date.</p> <p>2. Review existence of supporting documentation</p> <p>a. For a DITSCAP accredited system, review a copy of the System Security Authorization Agreement (SSAA).</p> <p>b. For a DIACAP accredited system, review the System Identification Profile (SIP), DIACAP Implementation Plan (DIP), DIACAP Scorecard, POA&amp;M, and related artifacts.</p>		
44. Has the sponsored PEO/PM information system or locally-developed information system been tested for compliance with the DODI 8500.2 requirements by an authorized Agent of the Certification Authority (ACA)?	AR 25-2 Para. 5-1(c); DoDI 8500.01E, DoDI 8500.2; DoDI 8510.01 DIACAP; Army Information Assurance Certification and Accreditation BBP, Agent of the Certification Authority (ACA), Para. 14.A	<p>1. Ask for the DIACAP Scorecard and review for validation results.</p> <p>2. Compare applicable IA controls listed on DIACAP scorecard with those in DODI 8500.2 (available on the DIACAP portal at <a href="https://diacap.iportal.navy.mil">https://diacap.iportal.navy.mil</a>).</p>		
45. Have the results from the testing been analyzed, CAT I weaknesses mitigated, and mitigating actions for CAT-II and CAT-III weaknesses captured in the Plan of Action and Milestones (POA&Ms) as required?	AR 25-2 Para. 5-2(h); DoDI 8500.01E; DoDI 8500.2; DoDI 8510.01 DIACAP, Para. 6.3.3.2.6.1.2, 6.3.3.1.6.1.3, and 6.3.3.2.6.1.4	<p>1. DIACAP Scorecard does not show any CAT I findings.</p> <p>2. Any Non-Compliance (N/C) results on the scorecard have been captured as line items in the POA&amp;M.</p> <p>3. Mitigation plan and dates have been captured in the POA&amp;M for each line item.</p> <p>4. Mitigation dates are prioritized by the highest CAT level and Impact Code.</p>		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Federal Information Security Management Act</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
46. Is there a contingency plan in place for each locally developed system (a single Information System or Network) as appropriate for essential functions and critical assets identified by the Commander?	AR 25-2, Para. 4-5i, DA PAM 25-1-2, Para.2-5a(2); DoDI 8500.2 IA Controls CODP and COEF	<p>1. Determine if a written contingency plan exists, is complete, is disseminated to appropriate elements within the organization, and is reviewed and approved by the Commander.</p> <p>2. Examine the contingency plan to determine if it meets all required IA contingency planning controls.</p>		
47. Have all locally developed systems had their Contingency Plans tested in the last year (MAC-II or MAC-III); or within the last six months (MAC-I)?	AR 25-2, Chap 4-5i; DoDI 8500.2, Section E4.A1; DA PAM 25-1-2, Para. 2e(2); DoDI 8500.2 IA Control COED-1	<p>1. Review Contingency Plan Testing information in APMS. (Fields: Accreditation Required, Contingency Plan Test Date).</p> <p>2. Review documented evidence of Contingency Plan scheduling and testing (e.g. Memorandum For Record, After Action Review, etc.).</p>		
48. Have Plans of Action and Milestones (POA&Ms) been submitted to RCIO-K for all locally developed systems that require corrective action?	DoDI 8510.01 DIACAP; AR 25-2, Para. 5-6e; DoDI 8510.01, Para. 4-7, 6.3.2.4., 6.3.3.1.4, 6.3.4.3; Certification and Accreditation BBP, Para. 10 K, L(1), M	<p>1. Review Annual Security Review information in APMS. (Fields: Accreditation Required, Annual Security Review Date)</p> <p>2. Review documented evidence of POA&amp;Ms for corrective actions.</p>		
49. Does the organization train personnel in their contingency roles and responsibilities?	AR 25-2, Para. 4-5i; DA Pam 25-1-2, Para. 2-4e(5)(a) and 3-4e; AR 500-3, 1-4f and 2-10a; DoDI 8500.2 IA Control PRTN, COTR, and COED	Review training records and contingency plan testing results to validate training of appointed personnel during contingency plan tests conducted every year (MAC-II or MAC-III) or every six months (MAC-I).		
50. Does the organization adequately provide physical and technical protection for backup and restoration assets to include backup copies of the operating system and other critical software (to include router tables, configuration settings, and security-related software)?	AR 25-2, Para. 4-5i; DoDI 8500.2 IA Control COBR and COSW	Validate that recovery media is actually stored off-site at a location detailed in the Contingency Plan. This validation can be performed by examining an SLA or MOU/MOA that states the protection levels of the data and how it should be stored.		
51. Has the organization identified an Alternate Site as part of its contingency plan?	AR 25-2, Para. 4-5i; DoDI 8500.2 IA Control COAS	<p>1. Interview IA personnel and examine continuity plan to ensure the following alternate processing site items have been addressed:</p> <p>a. The restoration of critical assets and the required mission and/or business essential functions as required by MAC level. For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.</p> <p>b. Examine the SLA or MOU/MOA for the alternate site to ensure alternate site security requirements are addressed.</p> <p>c. Necessary equipment and supplies are either in place or contracts are in place to resume operations.</p>		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

<b>Federal Information Security Management Act</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
52. Does the organization conduct data backups as required for the appropriate MAC level?	AR 25-2, Para. 4-5i; DA Pam 25-1-2, Para. 2-3d(2), DoDI 8500.2 IA Control CODB	1. Validate that backup and recovery procedures exist for the appropriate MAC Level.		
		2. Verify that the organization is completing the data backups as required for that system's MAC Level.		
		3. Verify that data backups (recovery media) are stored off-site at an alternate location using the same level of protection as primary site.		
53. Has the organization documented and tested the necessary secure recovery procedures?	AR 25-2, Para. 4-5i; DoDI 8500.2; DODI 8500.2 IA Control COTR-1, COPS, COMS, COSP	1. Verify that the contingency plan or the plan references another document that includes detailed step-by-step procedures needed for secure recovery. For Lab tested systems ensure this requirement is addressed in the PM's deployment plan. E4.A2, and E4.A3)		
		2. Verify Contingency plan test results indicate that the organization tests system/network restoration.		
		3. Verify that maintenance support for key IT assets available to respond within 24 hours (MAC-III) or available 24x7 to respond immediately upon failure (MAC-I or MAC-II)		
		4. Verify that maintenance spares and spare parts available within 24 hours (MAC-II or MAC-III) or available 24x7 immediately (MAC-I) upon failure.		
		5. Verify that continuous or uninterrupted power to key IT assets is available. For Lab tested systems ensure this requirement is addressed in the PM's deployment plan.		
		6. Examine SLA and MOU/MOA and vendor agreements to ensure the provided trusted recovery requirements are addressed.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Wireless Security</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
54. Are all unauthorized WLAN devices immediately removed/shut down and reported to the DOIM/RCERT?	AR 25-2, 4-20d(3) and 4-30a; Army Wireless Security Standards BBP Para. 5-B(4); DoDI 8500.2 IA Control ECWN	Review documented actions where unauthorized wireless devices were immediately removed from service.		
55. Are all known/trusted WLAN devices/systems properly accredited (NCP/TSP)?	AR 25-2 Para 3-2d(13) and 4-30a and b, and Para. 5; Army Wireless Security Standards BBP, Para. 5-K(4); DoDD 8100.02 Para 4.1	Validate that accreditation documentation includes all accredited WLAN devices / systems.		
56. Are all known / trusted WLAN assets accounted for in the Asset and Vulnerability Tracking Resource (A&VTR)?	AR 25-2, Para. 4-25a through e	Validate that accredited WLAN assets are listed in the A&VTR database.		
57. Are approved wireless IA tools (encryption, WIDS, access control) used to secure approved / accredited wireless LAN devices / architectures?	AR 25-2, Para. 4-1.d and 4-5i; Army Wireless Security Standards BBP, Para. 5-B(4), Para. 5-F(1); IA Tools BBP, Para. 4, 10, and 11; DoDI 8500.2 IA Control DCAS and ECWN	<p>1. Compare the IA tools / mechanisms used to secure the accredited WLAN devices / architectures with those listed on the Army Information Assurance Approved Products List (AIAAPL). <a href="https://informationassurance.us.army.mil">https://informationassurance.us.army.mil</a></p> <p>2. Ensure only approved IA tools are used to secure the WLAN devices / architectures.</p> <p>3. If the organization requires an IA tool that is not on the AIAAPL, they requested a Certificate of Networthiness prior to implementation.</p>		
58. Are approved encryption mechanisms in place for all approved / accredited WLAN devices connected to the installation network(s)?	AR 25-2, Para. 6-1; DoDD 8100.2, Para. 4.1.2. through 4.1.3; Army Wireless Security Standards BBP, Para. 5-F; DoDI 8500.2 IA Control ECCT	Verify that approved WLAN devices / architectures are equipped with FIPS 140-2 / NIST certified cryptographic mechanisms and are activated.		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

Portable Electronic Devices				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
59. Are all Portable Electronic Devices (PEDs) (specifically two-way wireless email devices (TWEDs) which connect to the network) used and procured by the organization since 31 Oct 03, on the Listing of Army-approved TWEDs?	Memorandum, CIO/G-6, "Guidance for Transition to S/MIME-Enhanced and CAC-Enabled TWEDs"; Memorandum, CIO/G-6, "Updated Two-way Wireless Email Device (TWED) Guidance"; Listing of Army-Approved Two-Way Wireless Email Devices (For New Procurements); DoDI 8500.2 IA Control DCAS	1. Print latest copy of the TWED Listing, from the Army Information Assurance Approved Products List (AIAAPL). - <a href="https://informationassurance.us.army.mil/ia_tools/IAProducts.xls">https://informationassurance.us.army.mil/ia_tools/IAProducts.xls</a> , and compare the list of IA and IA-enabled COTS products incorporated into the organization's system with the list of products from the AIAAPL.  2. If products are not present on the list, the unit should have a waiver from OIA&C authorizing use of the product.		
60. Are all PEDs, such as BlackBerry devices, protected with a 5 character minimum alphanumeric password?	Memorandum, CIO/G-6, 22 Jul 04, (allows for a limited exception for older CAC-enabled BlackBerry devices running pre-4.0 OS); DISA Wireless STIG; Associated BlackBerry Security Checklists; DoDI 8500.2 IA Control IAIA	1. Check BlackBerry Enterprise Server (BES) for group policy.  2. If available, spot check individual PEDs to see if they are configured to require a password.  3. Have user access their PED and check for number of characters to ensure it meets requirement.  4. Have user input wrong password to determine the maximum number of password attempts from the screen (i.e. 1 of 5).		
61. Are TWEDs used by GOs/SEs in the organization CAC-enabled?	Memorandum, CIO/G-6, 19 Aug 05, subject: "Updated TWED Guidance", Enclosure 4	1. Check BES for implementation of PKI/CAC.  2. If available, conduct a visual inspection of TWEDs used by a few of the GOs/SEs in the organization to verify compliance.(i.e. ask to "see the CAC reader for this device").		
62. Are unused/unauthorized wireless capabilities (e.g. Bluetooth voice profiles, built-in wireless capabilities of classified devices, etc.) of PEDs disabled prior to issue to end users?	Memorandum, CIO/G-6, 1 Aug 06, subject: "Updated Guidance on the Management of BlackBerry Devices with Internal Bluetooth Capability"; DoDI 8500.2 IA Control ECWN	1. If the organization is using BlackBerry devices, ask to see a policy dump from the BlackBerry Enterprise Server administrator (BES) to verify the "Headset" and "Handsfree" Profiles are disabled  a. Verify if Bluetooth is enabled (to support an approved Bluetooth Smart Card Reader (SCR)), or that Bluetooth is disabled entirely.  2. If Bluetooth-capable BlackBerry devices are being used by the organization but a SCR is not being used, confirm that Bluetooth cannot be turned on by the end user in the options menus.		
63. Are mobile computing devices configured in accordance with applicable security guides (i.e. DISA STIGs or NSA guides)?	AR 25-2, Para. 4-29; DoDI 8500.2 IA Control ECSC; BBP Data-At-Rest (DAR) Protection, Para. 8-E; appropriate DISA STIGs and/or NSA SNAC Guides	1. Conduct visual check of PEDs to validate compliance.  2. Ensure that employee owned information system (PEDs) are not connected to the network/Mobile Computing Devices.		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

<b>Portable Electronic Devices</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
64. Are laptops and other portable devices properly configured with an Army approved Data-At-Rest (DAR) solution?	AR 25-2, Para. 4-5j(6); CIO/G6 Memo Data at Rest (DAR) Memo; Data at Rest BBP; OMB Memorandum - M06-16, Subject: Protection of Sensitive Agency Information; DOD CIO PII Memorandum, 18 August 2006; VCISA ALARACT, dated 10 Oct 2006; DoDI 8500.2 IA Control ECCR	1. Conduct visual check of PEDs to validate that a DAR solution has been implemented and PEDs are appropriately marked/labeled.  2. Compare the employed encryption method with the current list of authorized DAR solution products <a href="https://informationassurance.us.army.mil/ia_tools/IAProducts.xls">https://informationassurance.us.army.mil/ia_tools/IAProducts.xls</a>  3. Confirm that the encryption tools are installed and enabled on all selected applications/devices		
65. Have all users of PEDs been properly trained on DAR protection requirements and user responsibilities?	AR 25-2, Para. 4-29d: BBP Data-At-Rest (DAR) Protection, Para. 8-B	Check organizational training documentation to see if training is being conducted.		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

<b>Army Web Risk Management</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
66. Are all organization's publicly accessible websites hosted on the ".mil" domain?	DA Pam 25-1-1, Para. 8-1d; AR 25-1, Para. 6-4n(11); Office of Management and Budget (OMB) Memorandum dated 17 DEC 2004, Para. 6a.	Verify that the website is on a ".mil" domain by going to the homepage or have a valid waiver present.		
67. Is operational information purged from publicly accessible Web sites?	AR 25-1, Appendix C	Operation information is defined in AR 25-1, Appendix C, C-4e(32)		
68. Are operational security tip-off indicators in the following categories purged from the organization's publicly accessible Web site?	AR 25-1, Appendix C	Operational security tip-off indicators are defined in AR 25-1, Appendix C, C-4e(33)		
69. Has the Web site reviewer performed a key word search for and subsequently removed sensitive personal or unit information from publicly accessible Web sites?	AR 25-1 Appendix C	Documents with sensitive information are listed in AR 25-1, Appendix C, C-4e(34)		
70. Does the organization ensure their public and private web site(s) are registered in A&VTR and posted on the Army "A-Z" page (www.army.mil/A-Z)?	DA Pam 25-1-1, Para. 8-1e	Verify that a website is registered by conducting a search of the Army A-Z listing on the Army Home page.		

**Eighth US Army Information Assurance Command Inspection Checklist**

1 MAY 09

<b>Personally Identifiable Information</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
71. Has the organization (i.e. Data Owners) identified all PII, evaluated the risk of loss or unauthorized disclosure, assign Impact Categories for electronic PII records, and established appropriate protection measures?	DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII; DoDD 5400.11, DoD Privacy Program	1. Review command, installation, agency documentation and written procedures that identifies all PII, assigns Impact Categories for PII electronic records, and established protective measures.  2. Query user population to assess user awareness of what PII is and how to protect it.		
72. Does the command, installation, agency, or activity have written procedures for incident reporting and notification when PII is lost, stolen, or otherwise available to individuals without a duty related, official need to know?	ALARACT 167/2007, VCSA SENDS: PII Incident Reporting and Notification Procedures; DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII; DoDD 5400.11, DoD Privacy Program	1. Review the organization's PII reporting procedures.  a. Verify guidance directs reporting of PII breaches/compromises to the US-CERT within one hour of discovery.  b. Verify guidance requires incidents be reported to CERT, and to agencies responsible for multiple reporting (i.e., Privacy Officials and FOIA staff) and that if the breach involves government credit card data, the issuing bank must be notified.  2. Query user population to assess user awareness of how to report the breach/compromise of PII.		
73. Have IA personnel incorporated protection measures for PII into the DIACAP process (NCP/TSP)?	DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII; DoDD 5400.11, DoD Privacy Program	Review the organization's DIACAP package (NCP/TSP) to determine if PII protection is incorporated into the security requirements.		
74. Has the organization established logging and tracking procedures for High Impact PII records on mobile computing devices or portable media that are removed from the government workplace?	DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII; DoDD 5400.11, DoD Privacy Program	1. Visit work locations where High Impact PII records are processed/stored.  2. Review evidence of logging and tracking of mobile devices and portable media containing High Impact PII records (e.g. G-1/S-1/DHR, G-3/S-3/DPTMS, G8/DRM/DMPO)		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Minimum IA Technical Requirements</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
75. Does the organization review for and verify dormant user accounts (i.e. remove departing users' accounts prior to departure, or terminating accounts which are verified inactive more than 45 days)?	AR 25-2, Para. 3-3a(10); Army Password Standards BBP; DoD 8500.2 IA Controls IAAC and IAIA	<ol style="list-style-type: none"> <li>1. Interview the IA personnel to verify documented operating procedures exist addressing user and system account creation, termination, and expiration.</li> <li>2. Verify status of assigned personnel to ensure accounts for departed personnel have been disabled/deleted.</li> </ol>		
76. Does the organization enforce separation of duties, role-based access, and least privilege through assigned access authorizations?	AR 25-2, Para. 4-5c; DoDI 8500.2 IA Control ECAN, ECLP, and IAIA	<ol style="list-style-type: none"> <li>1. Obtain a list of all privileged users and verify that these individuals possess a non-privilege and privilege account within the user account database.</li> <li>2. Ask for a list of functions performed on the network and the accounts used for these functions.</li> <li>3. Determine if the number of accounts is sufficient for the number of required functions.</li> </ol>		
77. Does the organization's standalone information systems automatically lockout access after a maximum of fifteen (15) minutes of inactivity?	AR 25-2, Para. 4-5 c(8); DoDI 8500.2 IA Control PESL	For standalone systems, review security policy on local system.		
78. Does the organization document, monitor, and control all methods of remote access (TSACS, VPN, etc.) to the information including remote access for privileged functions?	AR 25-2, Para. 4-5d; DISA Secure Remote Computing STIG; DoDI 8500.2 IA Controls EBRP, EBRU, and EBVC	<ol style="list-style-type: none"> <li>1. Obtain a list of remote access devices used by the organization (should be on the hardware/software list from the network accreditation).</li> <li>2a. Review audit logs and compare indicated users against signed remote user access agreements.</li> <li>2b. Review local policy/procedure for reviewing and configuration of audit logs.</li> <li>3. Review IDS logs for VPN activity</li> </ol>		
79. Does the organization implement virus protection which provides real-time protection and automated updates?	AR 25-2, Para. 4-5 (n); DoDI 8500.2 IA Control ECVP	Verify standalone systems have antivirus software installed and review system configurations in accordance with success measures.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Minimum IA Technical Requirements</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
<p>80. Do network devices comply with DoD ports, protocols, and services guidance?</p> <p><b>TACTICAL SYSTEMS ONLY</b></p>	AR 25-2, Para. 4-20d(4); DoDI 8500.2 IA Control DCPD	Check configuration tables, review active PPS, and compare with the most recent guidance.		
<p>81. Does the organization's information system enforce the use of firewalls and routers with access control lists (ACLs) to control the flow of information within the system and between interconnected systems in accordance with applicable policy?</p> <p><b>TACTICAL SYSTEMS ONLY</b></p>	AR 25-2, Para. 4-20e(1 and 2); DoDI 8500.2 IA Control ECIC	<p>1. Review network topology and configuration documentation.</p> <p>2. Review firewall rules and router Access Control Lists (ACLs).</p>		
<p>82. Are communications at the external boundary of the information system and at key internal boundaries within the system monitored and controlled?</p> <p><b>TACTICAL SYSTEMS ONLY</b></p>	AR 25-2, Para. 4-20d; DoDI 8500.2 IA Control EBBD	<p>1. Review network topology and configuration documentation</p> <p>2. Review firewall log and rule set.</p> <p>3. Review IDS log.</p> <p>4. Review router log and Access Control List (ACL).</p>		
<p>83. Does the organization ensure that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements?</p>	AR 25-2, Para. 4-3a(7); DoDI 8500.2 IA Control DCDS	<p>1a. Obtain a list of all outsourced dedicated IA services (IDS configuration, incident analysis and response, firewall operation, key management, etc.) from the System Owner.</p> <p>1b. Obtain copies of the risk analysis reports.</p> <p>2. Review scope of policies and procedures, training and certification documents, signed user agreements (both privileged and non-privileged), forms DD-254, and Statement of Work.</p>		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Classified Systems Management</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
84. Do classified systems display the classification level on the desktop or login screen (for example, wallpaper, splash screen) when the device is locked or the user is logged on or off?	AR 25-2 Para. 4-16(f); DoDI 8500.2 IA Control ECML	Ensure classified systems are displaying the appropriate classification level for the information being processed or stored through observation.		
85. Are miscellaneous processing equipment (i.e. copiers, facsimile machines, peripherals, typewriters, word processing systems, etc.) appropriately labeled at the classification of the information being processed?	AR 25-2, Para. 4-17c(1-5); AR 380-5, Para 4-1 and 4-34a and b; DoDI 8500.2 IA Control ECML	Ensure miscellaneous processing equipment is appropriately labeled at the classification level of the information being stored or processed through direct observation.		
86. Are wired/wireless portable electronic devices (PEDs) prohibited from areas where classified information is discussed or electronically processed?	AR 25-2, Para. 4-29a and 6-5 a.; DoDD 8100.2 Para. (4.2) (4.3) (4.4); DoDI 8500.2 IA Control ECWN	1. Visually review documentation (posted signs, SOPs, etc.) in reference to policy. Random verification of policy enforcement by checking users.		
87. Are Wireless keyboards and mice using radio frequency (RF) protocols (such as the 802.11-based standards) prohibited unless they use FIPS 140-2 validated cryptographic modules (if non-NSI data is processed) or NSA Type 1 products (if NSI data is processed) and are they approved for use by the DAA?	Army BBP, Wireless Security Standards, Version 3.0	1. Perform random spot-checks for wireless keyboards and mice.  2. Review approval documents from DAA.		
88. Are Infrared (IF) wireless keyboards and devices approved by the DAA in consultation with the CTTA?		Perform random spot-checks on NIPRNet or SIPRNet systems (no mixing in same area). Review DAA approval documents and CTTA assessment results.		
89. Does the organization physically control and securely store information system media (paper and digital) based on the highest classification of information on the media to include pickup, receipt, transfer and delivery of such media to authorized personnel?	AR 25-2, Para. 4-16(a and b), DoD 5200.1-R, c7.2.1.1.4, c7.2.1.1.5, c7.2.1.2, c7.2.2, ap7.4.1; DoDI 8500.2 IA Control PESS	1. Interview the Security manager and tour the facility to verify that documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with regulation.  2. Review and validate media transport written requirements and procedures.		
90. Does the organization sanitize or destroy classified information system digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using the information contained on the media?	AR 25-2, Para. 4-18(b-j); AR 380-5, Para. 3-18; Reuse of Computer Hard Drives BBP; DoDI 8500.2 IA Control PECS	1. Interview the Security Manager to verify that procedures exist to clear and sanitize all documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense. Verify that the procedures are strictly enforced.  2. Request review of clearing/purging/declassifying/destruction records.  3. Verify that logs document that released equipment in the sample set was properly cleared, sanitized, and documented.		

**Eighth US Army Information Assurance Command Inspection Checklist**

**1 MAY 09**

91. Does the organization ensure only authorized maintenance personnel with a need-to-know are granted physical access to classified information systems?	AR 25-2, Para. 4-10 (d), AR 380-5, Para. 6-1; DoDI 8500.2 IA Control PRMP	Interview Security Manager to verify that physical access to the computing facility is granted only to authorized personnel with a need to know, proper background investigation and security clearance, and formal approval.		
---	---	---	--	--

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

<b>Classified Systems Management</b>				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
92. Does the organization ensure all classified removable media (Thumb Drives, floppies and CDs) and classified information systems comply with all requirements for marking and labeling contained in policy and guidance documents?	AR 25-2, Para. 4-17 (a-d); DoDI 8500.2 IA Control ECML	Look at classified removable media.		
93. Does the organization ensure devices that display or output classified information in human-readable form are positioned to deter unauthorized individuals from reading the information?	DoDI 8500.2 IA Control PEDI	1. Observe the placement of devices that display or output classified information in human- readable form and verify they are positioned to deter unauthorized individuals from viewing the information.  2. Verify that procedures are in place to black out viewable classified information or to position monitors/displays to deter viewing when unauthorized personnel are escorted in the immediate vicinity.		
94. If the organization holds a COMSEC account, has the Commander appointed a COMSEC Custodian and at least one Alternate?	AR 380-40, Para. 1-4h(1) and 2-2; DoDI 8500.2 IA Control ECCM	Review appointment orders to ensure they are current.		
95. Has the COMSEC Custodian and Alternate been trained and certified through the Standardized COMSEC Custodian Course?	AR 380-40, Para. 2-2b; DoDI 8500.2 IA Control ECCM	1. Review Standardized COMSEC Custodian Course (SCCC) Certificates.  2. If the COMSEC Custodian is not trained and certified or have a valid waiver, notify the CSLA P3 Team (DSN 879-2332, Cml (520)-538-2332). Comprehensive training and waiver requirements provided on attached documentation.		
96. For Army Key Management System (AKMS) accounts, have at least two personnel been formally trained on the local COMSEC Management Software (LCMS)?	AR 380-40, Para. 2-2b; DoDI 8500.2 IA Control ECCM	1. Review LCMS training Certificates.  2. If the COMSEC personnel are not trained and certified, notify the CSLA Tier 1 Operations (DSN 879 or Cml 520-538-8238).		
97. Does the organization ensure only approved Keyboard, Video, and Mouse (KVM) switch boxes are in use for switching between systems of different classification levels?	AR 25-2 Para. 4-20(h), KVM BBP; DoDI 8500.2 IA Control DCBP	Observe multiple classification systems at one or more workstations to verify authorized KVM is in use.		
98. Is the classified network transmission protected with NSA Type 1 Cryptographic devices and/or a compliant and approved Protected Distribution System (PDS) IAW AK Cir 25-10?	AR 25-2, Para. 6-3, NSTISSI 7003; IA Control ETCT; AK Cir 25-10	1. Verify encryption device is authorized and on approved list.  2. Inspect PDS to ensure standards are met and PDS is approved by the DAA.		

## Eighth US Army Information Assurance Command Inspection Checklist

1 MAY 09

Physical Security				
Question/Tasks	Authoritative Standards (Reference)	Validation	Assessment	
			Compliant	Non-Compliant
99. Does the organization have current signed procedures to control visitor access to critical IT infrastructure facilities (e.g. ADN, MCN, DCO, Server Room, Network Operations Center, etc), are detailed visitor logs being kept, and are entrances controlled during working hours and guarded or locked during non-work hours?	DoDI 8500.2 IA Controls PEPF and PEVC	1. Review the visitor access policy, access roster, and DA Form 1999 (Restricted Area Visitor Register).  2. If the facility processes classified information, verify the clearance level of authorized personnel and visitors with the facility Security Manager using either a Security Clearance Access Roster (SCAR) or visitation authorization (either memorandum or JPAS).		
100. Are daily security checks being made at the end of each workday (and non-workdays as required) and documented on a SF 701?	AR 380-5, Para. 6-11a; DoDI 8500.2 IA Control PESP	Review SF 701 in accordance with success measures.		
101. Have lock combinations been changed either within the past 12 months or upon departure of authorized personnel?	AR 380-40, Para. 4-5g; AR 380-5, Para. 7-8b and e	Review SF 700 in accordance with success measures.		
102. Are dates and times when unlocking and securing each security container appropriately recorded on a SF 702?	AR 380-5, Para. 6-10b	Review SF 702 in accordance with success measures.		
103. Is the MSC's primary C2 communication facility (bunker, EOC) designated as a Mission Essential Vulnerability Area (MEVA) and has a physical security inspection been conducted by the PMO in the past year?	AR 190-13, Para 1-24	Review PMO physical security inspections results (reports/memos).		
104. Is the designated MEVA included in the Installation's Physical Security Plan?	AR 190-13, Para 1-24	Review Installation Security Plan		
<p>Primary Inspector Name and Signature _____ Date: _____</p> <p>Unit POC: _____ Phone Number _____</p> <p>Email Address: _____</p>				