ROTC BRIGADE
ORGANIZATIONAL INSPECTION PROGRAM
INFORMATION SUPPORT ACTIVITY CHECKLIST
For use of this form, see Cdt Cmd Reg 145-8-4, the proponent agency is ATCC-IT

INFORMATION SUPPORT ACTIVITY

Revision Date: *11/8/2012*

Question	Authoritative Standards (Reference)	Yes	No	NA
Incident Handling				
1. Does the organization have an incident response plan? (NOTE: A tenant organization must have either their own incident response plan or a copy of the response plan developed by the service provider.)	AR 25-2, Para. 4-21; DoDI 8500.2 IA Control VIIR; CJCS Instruction 6510.01F			
2. Does the incident response plan establish a local incident response team; identifying key roles?	DoDI 8500.2 (DIACAP) IA Control VIIR & PRTN			
3. Does the incident response plan define reportable incidents?	AR 25-2, Para. 4-21c; DoDI 8500.2 IA Control VIIR; CJCSM 6510.01A			
4. Does the incident response plan address response to INFOCON measures?	DoDI 8500.2 IA Control VIIR; CJCSM 6510.01F Encl C, para 7; STRATCOM Directive 527-1 para 3.7.5			
5. Does the incident response plan provide for Incident Response Team training?	AR 25-2, Para. 4-21c; DoDI 8500.2 IA Control VIIR; CJCSM 6510.01A			
6. 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; DoDI 8500.2 IA Control VIIR			
7. 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			
8. Do IA personnel report information system security incidents, to include unauthorized disclosure of classified information, as required?	AR 25-2, Para. 3-2d(3), f(13), and 3-3a(14)			
9. 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			
10. Does the incident response plan include the recovery actions required prior to placing a compromised system back on the network?	AR 25-2, Para. 4-23a			

11. 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			
IA Training				
12. Does the BDE's IA user training program comply with the Army minimum training requirements?	AR 25-2, Para. 4-3a (8) a, 1-11; DoD 8570.1-M, Para. C6.2.5; DoDI 8500.2 IA Control PRTN			
13. Do all users complete initial IA Awareness training before receiving network access?	AR 25-2, Para. 4-3a(8)(a), NIST 800-53 Appendix F AT2, CJCSM 6510.01F Enclosure A, Para. 11, DoD 8570.1-M Para. C6.2.2; DODD 8570.1 5.9.2; DoDI 8500.2 IA Control PRTN			
14. Do all users complete refresher IA Training annually?	AR 25-2, Para. 4-3a (8)(b) , NIST 800-53 Appendix F AT2, CJCSM 6510.01F Enclosure A, Para. 11 CJCSM, DoD 8570.1-M Para. C6.2.2; DODD 8570.1 5.9.2; DoDI 8500.2 IA Control PRTN			
15. Have all IA personnel in Technical Levels I-III completed the Army required minimum training within six months of appointment to the position?	AR 25-2, Para. 4-3a(2), (6)(a-c); DoD 8570.1-M C3.2.3.1; IA Training and Certification Best Business Practice, Para. 10a, b, and c; Army CIO/G-6 MFR United States Army Information Assurance (IA) Military Workforce Certification Process, Jul 19 2011			
16. Have all IA personnel in Technical Levels I-III obtained the appropriate DoD IA baseline commercial certification within six months of appointment?	AR 25-2 4.3a(6)(a)&(d); DoD 8570.1-M C3.2.4.1.1, C.4.2.3.2,; IA Training and Certification BBP, Para. 10			

17. Have all IA personnel in Technical Levels I-III obtained the appropriate computing environment certification, within six months of appointment?	AR 25-2 4.3a(6)(a)&(d); DoD 8570.1-M C3.2.4.1.1; IA Training and Certification BBP, Para. 10; ALARACT 284/2011 - 011658Z Aug 11-COMPUTING ENVIRONMENT CE CERTIFICATIONS FOR THE ARMY INFORMATION ASSURANCE IA WORKFORCE			
18. Have all personnel that have privileged access as a local administrator or an OU administrator been appointed, trained, and certified as an IA Technical I-lll?	AR 25-2 Para. 3-3c(15) 4-3a(2), (6)(a-c); DoD 8570.1-M Para. C3.2.3., C1.4.4.4., C3.2.4.1.2.; DoDI 8500.2 IA Control PRTN; BBP 05-PR-M-0002			
19. Are all BDE user IA training records in Army Training and Certification tracking system (ATCTS)				
IA Program Management				
20. Are personnel required to sign a user agreement, and are privileged users additionally required to sign a Privileged-Level Access Agreement, prior to being granted access to the information system?	AR 25-2, Para. 3-3c(1), 4-3; DTM 08-060 Change 3; IA BBP 06-PR-M-0003 (Privileged-Level Access Agreement AUP), Para. 8; DoDI 8500.2 IA Control PRRB			
21. Are hard drives and solid-state drives (SSDs) that will be reused in a different Army or DoD environment purged with an approved Army wiping tool prior to release?	AR 25-2, Para. 4-18a, b, and d; IA BBP 03-PE-O-0002 (Reuse of Army Computer Hard Drives), Para. 7A(1); DoDI 8500.2 IA Control PECS-1 and PECS-2			
22. Are hard drives and solid-state drives (SSDs) that stored classified or sensitive information (e.g. non-public) degaussed with an NSA-approved degausser and destroyed using an NSA-approved destruction method? NOTE: This includes drives involved in an Unauthorized Disclosure of Classified Information (UDCI), commonly known as spillage.	AR 25-2, Para. 4-18, Glossary Section II; IA BBP 03-PE-O-0002 (Reuse of Army Computer Hard Drives), Para 7A(5); NSA/CSS Evaluated Products List - Degausser			

23. Are purged/destroyed hard drive actions documented on a disposition certification label AND in a Memorandum for Record (MFR)?	AR 25-2, Para. 4-18a; IA BBP 03-PE-O-0002 (Reuse of Army Computer Hard Drives), Para. 9A(5), 9B(9), and 9C(7)			
24. Is the Memorandum for Record (MFR) for hard drive and solid-state drive disposition retained for at least five years?	ARIMS RRS-A Record Number 25e; AR 25-2, Para. 4-18a; IA BBP 03-PE-O-0002 (Reuse of Army Computer Hard Drives), Para. 9A(5), 9B(9), and 9C(7)			
25. Do authorized users who are contractors, DOD direct or indirect hires, foreign nationals, foreign representatives, seasonal hires, temporary hires, or volunteers have their respective affiliations incorporated as part of their e-mail addresses?	AR 25-2 Para. 4-20f(8); ALARACT 021/2010; DoDD 8500.01E Para. 4.10; DoDI 8500.2 IA Control ECAD-1; CJCSI 6510.01F, Para. A-7c			
26. Do authorized users who are contractors, DOD direct or indirect hires, foreign nationals, foreign representatives, seasonal hires, temporary hires, or volunteers have their respective affiliations identified within their display names?	AR 25-2, Para. 4-15a and 4-20f(8); DoDI 8500.2 IA Control ECAD-1			
27. Do authorized users who are contractors, foreign nationals, foreign representatives, foreign officials, or foreign personnel have their respective affiliations indicated in an automatic signature block?	AR 25-2, Para. 4-15c; DoDI 8500.2 IA Control ECAD1			
28. Does management ensure that users understand that they have no reasonable expectation of privacy by enforcing the display and acceptance of the Notice and Consent Banner every time a user logons to an Army system?	AR 25-2 Para. 4-5.m; DoD DTM 08-060; DoDI 8500.2 IA Control ECWM; CJCSI 6510.01F, Para. A-9			
29. 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 ; CJCSI 6510.01F, Para. A-7; DoD 5220.22-M, Section 2			

30. Are there any outstanding waivers older than 6 months?	AR 25-2			
31. Has the appropriate authority formally appointed IA workforce personnel via appointment orders?	AR 25-2 Para. 2-24f and Chapter 3			
32. Are security clearance requirements included in all Statements of Work and all IT / IA contracts, to include maintenance contracts?	AR 25-2, Para. 4-10.a; DoDI 8500.2 IA Control PRAS-1 (Sensitive) or PRAS-2 (Classified); DoD 5220.22-M, Section 2			
33. Does the organization restrict the use of employee owned information systems (EOIS)?	AR 25-2, Para. 4-31; AR 25-1, Para. 6-1i			
34. Are leased copier contracts written to allow for the removal of hard drives before equipment is returned?				
35. Are all current hardware and software assets tracked and maintained?	AR 25-2, Para. 4-9.c, 4-28.h, and 4-28.j; DoDI 8500.2 IA Controls DCHW-1 and DCSW-1			
36. Does the organization ensure information systems and removable media comply with all requirements for marking and labeling?	AR 25-2, Para. 4-17; AR 380-5, Para. 4-32, 4-34, 5-3, 5-8, 5-12, 5-16, and 5-20; AR 380-5, Para. 4-34.b; AR 25-55, Para. 4-200d; DoDI 8500.2, Para. 5.12.5 and IA Control ECML; CJCSI 6510.01F, Para. A-6; DTM 04-009			
37. 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?	AR 25-1, Para. 5-1; AR 25-2, Para. 4-3a(7); DoDI 8500.2, Para. E3.4.5, IA Controls DCDS and DCIT; DoDD 8500.01E, Para. 4.2 and E2.1.16; CJCSI 6510.01F, Para. A-5, A-10; DFARS Part 239.74			

PKI				
38. Do all Soldiers, DA Civilians, eligible contractors, and foreign national employees who require logical access to the NIPRNET have a hardware token with identity, signature and encryption certificates?	Army CIO/G-6 ALARACT Army Accelerated Implementation Of Common Access Card Cryptographic Network Logon, Para 5.1.2.; JTF-GNO Communication Task Order 06-02, Para 6A.; NGB Memo Update ARNG VOLAC Pilot Memo dated 2010 07 (Jul) 14 ; DoDI 8500.2			
39. 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 ALARACT number 028-2006, 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			
40. Are all System Administrators using an Alternative Smart Card Logon (ASCL) Token to access their higher privileged account?	AR 25-2 Para 3-3a(13); 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			
41. Are Active Directory accounts for users with a CAC or ASCL token configured for user-based enforcement? (NOTE: Organization is compliant if they have a POA&M or waiver approved by Army CIO/G-6.)	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) and 5.2.2			

Wireless				
42. Are all unauthorized wireless devices (WLAN, RF keyboards, RF mice, Bluetooth devices, etc) immediately removed/shut down and reported to the DOIM/NEC/RCERT?	AR 25-2, 4-22 and 4-30a; Army Wireless Security Standards BBP Para. 5A(4); DoDI 8500.2 IA Control ECWN			
Portable Electronic Devices (PED)				
43. Are all Portable Electronic Devices (PEDs) used and procured by the organization on the Unified Capabilities Approved Products List (UCAPL)?	AR 25-2, Para. 4-29a-f; DoDI 8500.2 IA Control DCAS; DoDI 8100.04			
44. Does the organization configure portable devices (e.g., Blackberry, Apriva, etc.) in accordance with applicable security guides (i.e., DISA STIGs or NSA guides)?	AR 25-2, Para. 4-5.f(6), Para. 4-29; DoDI 8500.2 IA Control ECSC; appropriate DISA STIGS; Wireless BBP; DoDI 8100.02			
45. Are mobile devices (including laptop PCs) properly configured with an Army approved Data-At-Rest (DAR) solution?	AR 25-2, Para. 4-5j(6); Data at Rest BBP; OMB Memorandum - M06-16, Subject: Protection of Sensitive Agency Information; DOD CIO PII Memorandum, 18 August 2006; VCSA ALARACT, dated 10 Oct 2006; DoDI 8500.2 IA Control ECCR			
46. Are users aware of their responsibility to protect data stored on their PED?	AR 25-2, Para. 4-29d; BBP 06-EC-O-0008: Data-At-Rest (DAR) Protection, Para. 8-B; Applicable Wireless STIG/Checklist (i.e., BlackBerry, Windows Mobile)			
47. If the organization is not employing a whole disk DAR solution (laptops only) (e.g. Mobile Armor), are enterprise domains configured to support Encrypted File System (EFS) recovery agents and technically qualified EFS recovery agents been designated?	BBP 06-EC-O-0008: BBP Data-At-Rest (DAR) Protection Para. 8-I and 11-A(3); AR 25-1, AR 25-2			
48. Are mobile communications devices issued by BOI?				
49. Are computers secured to desks?				
50. Are cellular phones and blackberry devices recorded on a hand receipt?				

ROTC BRIGADE
ORGANIZATIONAL INSPECTION PROGRAM
INFORMATION SUPPORT ACTIVITY CHECKLIST
For use of this form, see Cdt Cmd Reg 145-8-4, the proponent agency is ATCC-IT

Army Web Risk Content Management				
51. Have the Commander, the Public Affairs Officer, OPSEC Officer, and the Webmaster properly cleared information posted to the WWW, and registered Army Social Networking Sites pertinent to the organization in areas accessible to all account types?	AR 25-1, Para. 6-7; AR 530-1; Army CIO/G6 - Responsible Use of Internet Based Capabilities Memorandum; Army Public Affairs Army Social Media Best Practices Document; U.S. Army Social Media Handbook January 2011			
52. Have all personnel appointed as OPSEC Officers, Webmasters, reviewers (to include PAO), and content managers received OPSEC web content vulnerability and web risk assessment training?	AR 530-1, Para. 4-3b(2); DA Pam 25-1-1, Para. 8-4b			
53. Has the organization conducted quarterly and annual reviews to ensure FOUO, FOIA-exempt, or other non-public information has been removed from and does not exist on the unit's publicly accessible website?	AR 25-1, Para. 1-7b and 6-7c(4) and Web site management control checklist (Appendix C) items 26-37; AR 530-1, Para. 2-3a(15a); DoD Web Site Admin Policy, Part II, Section 3.5.3; DoD 5400.7-R, Para. C3.2			
54. Are publicly accessible websites behind an Army Reverse Proxy Server?	AR 25-2, Para. 4-20g(12) & (13); AR 25-1, Para. 6-7c(6a); DoD Internet - NIPRNet DMZ STIG			
55. Is this publicly accessible website 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.			
56. Are the unit's publicly accessible telephone directories generic? (Such as no names or personally identifying information.)	AR 25-1, Para. 6-4 r(1)			
57. Does the organization ensure their public web site(s) are registered and posted on the Army "A-Z" page (www.army.mil/info/a-z)?	DA Pam 25-1-1, Para. 8-1e			

58. Have all private (non-public) web sites been configured to require, at a minimum, Class 3 DoD PKI certificates for identification and authentication?	AR 25-2 Para. 4-20 g(14); ALARACT 180/2006, Para. 4A1& 4B; DoDI 8500.2 IA Control IATS			
59. Does the organization ensure Army Social Networking site(s) are properly registered through the Army.mil website?	AR 25-1, Para. 6-7; AR 530-1; Army CIO/G6 - Responsible Use of Internet Based Capabilities Memorandum; Army Public Affairs Army Social Media Best Practices Document; U.S. Army Social Media Handbook January 2011			
Personal Identifiable Information (PII)				
60. Has the organization assessed the likely risk of harm caused by the breached information and then assess the relative likelihood of the risk occurring (risk level) for making the determination whether notification to affected individuals is required?	DoD Memorandum, Subject: Safeguarding Against and Responding to the Breach of PII 05 Jun 09 (Part I b pg 2 & Table 1 Appx A); DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII 18 Aug 06 (Para 4.1)			
61. Does the organization have written internal command procedures for incident reporting and notification when PII is lost, stolen, or otherwise disclosed to individuals without a duty related, official need to know?	ALARACT 050/2009, PII Incident Reporting and Notification Procedures (Para 4.3); DoD Memorandum, Subject: Safeguarding Against and Responding to the Breach of PII 05 Jun 09 (Part IV, Pg 9); DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII 18 Aug 06 (Para:4.3)			
Minimum Information Assurance (IA) Technical Requirement				
62. 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			

ROTC BRIGADE
ORGANIZATIONAL INSPECTION PROGRAM
INFORMATION SUPPORT ACTIVITY CHECKLIST
For use of this form, see Cdt Cmd Reg 145-8-4, the proponent agency is ATCC-IT

Classified Systems Management				
63. 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			
64. Are miscellaneous processing equipment appropriately labeled (i.e. copiers, facsimile machines, peripherals, typewriters, word processing systems, etc.)?	AR 25-2, Para. 4-17c(1-5), 4-32 Miscellaneous processing equipment; AR 380-5, Para 4-1 and 4-34a and b; DoDI 8500.2 IA Control ECML			
65. Are 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; Wireless Security Standards BBP Para K(3)			
66. 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); AR 380-5 Section II; 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			
67. 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); Reuse of Computer Hard Drives BBP; DoDI 8500.2 IA Control PECS			
68. Does the organization ensure only authorized IT 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			
69. Does the organization ensure all classified removable media (Thumb Drives, floppies, USB hard drives, CDs, etc.) and classified information systems comply with all requirements for marking and labeling?	AR 25-2, Para. 4-17 (a-d); AR 380-5, Para. 4-33; DoD 5200.1-R, Para. C5.4.9 and C5.4.10; DoDI 8500.2 IA Control ECML; BBP 03-PE-O-0004			

ROTC BRIGADE
ORGANIZATIONAL INSPECTION PROGRAM
INFORMATION SUPPORT ACTIVITY CHECKLIST
For use of this form, see Cdt Cmd Reg 145-8-4, the proponent agency is ATCC-IT

70. 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			
71. Is unattended classified information (to include IS media and keyed Controlled Cryptographic Items) stored in either a GSA Approved container or approved open storage area?	AR 380-5 para 7-4a; TB380-41 para 5.3			
GENERAL				
72. Are results of your subordinate unit's OIP latest inspections and corrective actions on file?	(AR 25-400-2, Table B-9, FN: 20-1a)			
73. Are the results of the BDE's last OIP inspection on File?				
74. Is excess unused equipment turned in/disposed of timely and properly?				
75. Is the BDE using best practices to reduce cost of printing? (network printers instead of standalone printers)				
76. Are users encrypting all e-mails that contain sensitive or critical information?	TRADOC Supplement 1 to AR 25-2			
77. Are sensitive documents destroyed in an appropriate manner?	AR 380-5- chapter 3			
78. Are CACs being left in computers while users are away from computer?				
79. Is HSS and account information in IMS Accurate?				
Records Management				
80. Has a Records Management Coordinator been appointed within the Brigade?	AR 25-400-2, para 1-4			
81. Are all files maintained under the Army Records Information Management System (ARIMS)?	AR 25-400-2			
Publications and Forms Management				
82. Are locally produced forms reviewed to ensure they do not duplicate the functions of higher echelon forms?	AR 25-30, para 3-14-2			

ROTC BRIGADE
ORGANIZATIONAL INSPECTION PROGRAM
INFORMATION SUPPORT ACTIVITY CHECKLIST
For use of this form, see Cdt Cmd Reg 145-8-4, the proponent agency is ATCC-IT

Mail and Distribution				
83. Has an official mail control officer been appointed in writing by the current brigade command?	AR 25-51,para 1-6			
84. Is the official mail control officer aware of limitations on and the use of special postage services?	AR 25-51, para 1-5			
85. Is mail being sent in the most economical way?	AR 25-51			
86. Is the brigade maintaining mail expenditure records and reporting quarterly or as directed by their higher headquarters expenditures using DA Form 7224-R (Quarterly Positive Accountability Postage Administration System)?	AR 25-51, para 2-9			
87. Is the brigade maintaining record of private carrier expenditures using DA Form 7224-2-R?	AR 25-51, para 2-9			