SECRETARY OF THE ARMY
WASHINGTON

2 8 OCT 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2013-22 (Implementation and Enforcement of the Army Information Assurance Program)

1. References:

a. Army Regulation (AR) 25-2 (Information Assurance), 24 October 2007, Rapid Action Revision Issued 23 March 2009.

b. Memorandum, Under Secretary of the Army, 15 May 2013, subject: Implementation Plan for Army Headquarters Transformation.

2. In accordance with AR 25-2, commanders, directors and managers are responsible for implementing and enforcing the Army Information Assurance (IA) Program within their respective commands and activities.

3. To help enforce compliance with IA, the Army Chief Information Officer (CIO)/G-6 has established and will serve as the proponent for the governance process for Army IA risk management effective immediately. As part of this process, the CIO/G-6 will assume responsibility for executing IA compliance inspections, pursuant to the 15 May 2013 transfer of responsibility from The Inspector General (reference 1b).

4. All Headquarters, Department of the Army Principal Officials, commanders, Army organizations and personnel will support the CIO/G-6 in executing the requirements set forth in this directive and implementing the governance process for Army IA risk management.

5. This process will provide the governance structure and procedures for assessing, managing and reducing Army IA risks. It will leverage existing Federal, Department of Defense, Joint and Army IA inspection and assessment programs to identify the primary IA threats to the Army's Network, Warfighting and Business Mission Areas. Stakeholders across the Army IA community of practice will share information and lessons learned, and collaborate to identify and resolve systemic IA vulnerabilities through existing business processes.

6. The CIO/G-6 will implement the governance process and oversee its maturation. Headquarters, Department of the Army Principal Officials; commanders of Army Commands, Army Service Component Commands and Direct Reporting Units; and

other key business process owners will help the CIO/G-6 implement and refine the process in accordance with the enclosure.

7. The Inspector General will conduct oversight inspections of the Army IA Program, including the risk management governance process, organizational IA programs and systemic inspections (as directed), to determine the effectiveness of such programs.

8. This directive supplements the policies and procedures set forth in AR 25-2. Any part of AR 25-2 determined to be inconsistent with the provisions of this directive is hereby superseded. Applicable provisions of this directive will be incorporated into the next revision of AR 25-2.

John M McHugh

Encl

John M. McHugh

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Pacific
U.S. Army Europe
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Africa/Southern European Task Force
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Installation Management Command
(CONT)

DISTRIBUTION: (CONT)
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade

CF:
Director, Army National Guard
Director of Business Transformation

GOVERNANCE PROCESS FOR ARMY INFORMATION ASSURANCE RISK MANAGEMENT

1. Cyber attacks threaten the Army network and its information every day, putting our operations and personnel at risk. Insider threats, whether malicious or unintentional, pose significant danger, as demonstrated by incidents that have resulted in the unauthorized and negligent disclosure of sensitive Army data and personally identifiable information. Commanders, directors and managers can significantly mitigate our vulnerability to these threats by implementing and enforcing the Army Information Assurance (IA) Program within their respective commands and activities.

2. IA must be integral to all Army operations, missions and functions. Commanders, leaders and managers are responsible for adopting and instituting behavior-changing practices necessary to safeguard information, information technology capabilities and personnel. They must:

a. incorporate IA into their risk-management processes to ensure that their network, warfighting and business mission information and systems are protected.

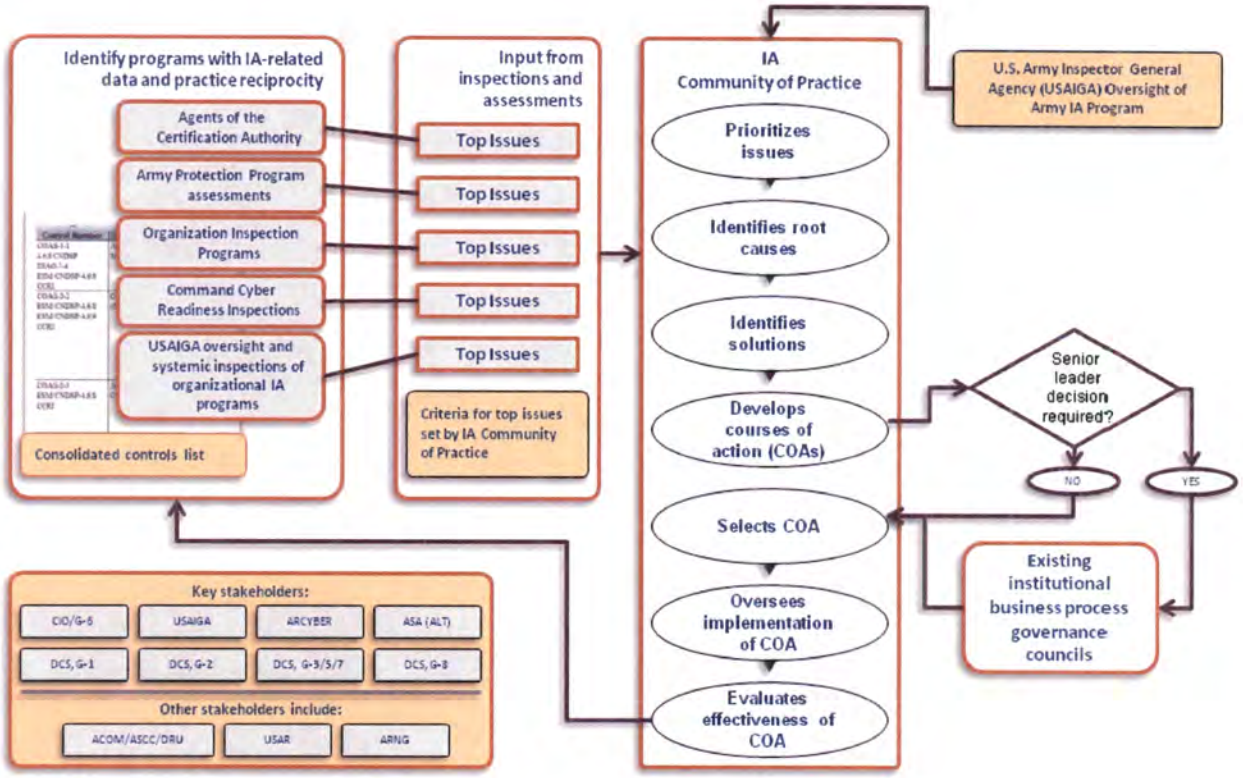
b. ensure that personnel are responsible for daily practices that protect information and information technology capabilities. IA must receive the same attention as safety in planning and mission execution.

c. assess mission capability and make sure all practices are compliant with IA policies, processes and standards. IA must be linked to mission readiness.

3. To help commands and activities enforce compliance with IA, the Army Chief Information Officer (CIO)/G-6 has established and will serve as the proponent for the governance process for Army IA risk management. The process provides the governance structure and steps for assessing, managing and reducing Army IA risks. It will leverage existing Federal, Department of Defense (DoD), Joint and Army IA inspection and assessment programs to identify the primary IA threats to the confidentiality, integrity and availability of Army information. Stakeholders across the Army IA community of practice (CoP) will share information and lessons learned, and collaborate to identify and resolve systemic IA vulnerabilities through existing business processes.

4. The Army CIO/G-6 provides general oversight for the Army IA risk management process (shown in the figure on the next page). Headquarters, Department of the Army, including key business-process proponents (for example, in resource planning and policy development); Army Commands; Army Service Component Commands; and Direct Reporting Units will help the CIO/G-6 implement and refine the IA risk management process in a manner that effectively and efficiently leverages existing business processes.

Governance Process for Army IA Risk Management


Identify programs with IA-related data and practice reciprocity
Agents of the Certification Authority
Army Protection Program assessments
Organization Inspection Programs
Command Cyber Readiness Inspections
USAIGA oversight and systemic inspections of organizational IA programs
Consolidated controls list
Input from inspections and assessments
Top Issues
Top Issues
Top Issues
Top Issues
Top Issues
Criteria for top issues set by IA Community of Practice
IA Community of Practice
Prioritizes issues
Identifies root causes
Identifies solutions
Develops courses of action (COAs)
Selects COA
Oversees implementation of COA
Evaluates effectiveness of COA
U.S. Army Inspector General Agency (USAIGA) Oversight of Army IA Program
Senior leader decision required?
NO
YES
Existing institutional business process governance councils
Key stakeholders:
CIO/G-6
USAIGA
ARCYBER
ASA (ALT)
DCS, G-1
DCS, G-2
DCS, G-3/5/7
DCS, G-8
Other stakeholders include:
ACOM/ASCC/DRU
USAR
ARNG

Abbreviations Used:

ACOM	= Army Command
ASA (ALT)	= Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ARCYBER	= U.S. Army Cyber Command
ARNG	= Army National Guard
ASCC	= Army Service Component Command
DCS	= Deputy Chief of Staff
DRU	= Direct Reporting Unit
USAR	= U.S. Army Reserve

5. The Army IA CoP, led by the CIO/G-6 Director of Cybersecurity, will execute the Army IA risk management process. The Army IA CoP is composed of appropriate representatives from key business processes and operational stakeholders, including but not limited to, the:

- Assistant Secretary of the Army (Acquisition, Logistics and Technology);
- Inspector General;
- Deputy Chief of Staff, G-1;
- Deputy Chief of Staff, G-2;
- Deputy Chief of Staff, G-3/5/7;
- Deputy Chief of Staff, G-8;

- Commander, U.S. Army Forces Command;
- Commander, U.S. Army Training and Doctrine Command;
- Commander, U.S. Army Materiel Command;
- Commander, U.S. Army Cyber Command;
- Chief, Army Reserve; and
- Director, Army National Guard.

6. Other business process proponents will participate in the Army IA risk management process as necessary to help develop and implement cost-conscious, effective and efficient remediation courses of action (COAs).[1]

a. The first step in the Army IA risk management process is to identify existing inspection and assessment programs that generate IA-related data. The CIO/G-6 will notify proponents whose programs meet this criterion and familiarize them with the risk management process and their role in it. The process will leverage the inspection data to identify systemic deficiencies that put Army information at significant risk. The IA CoP will oversee implementation of a consolidated IA inspection and assessment checklist that will map that data to respective programs, as well as standardize outcomes for similar inspection and assessment activities. Use of a consolidated checklist will ensure that trusted and assured data will be available for inspection and assessment programs to share and reuse as appropriate.

b. Existing inspection and assessment programs that generate IA-related data include, but are not limited to:

(1) U.S. Army Audit Agency audits, which are topic-specific information technology audits based on previous audit work, leadership direction and high-risk areas, such as cyber security and enterprise services.

(2) DoD Information Assurance Certification and Accreditation Process (DIACAP) Scorecards, which are system-focused, third-party validations conducted by agents of the certification authority as part of the IA certification and accreditation process (in accordance with DoD Instruction 8510.01 (DoD Information Assurance Certification and Accreditation Process (DIACAP)) and AR 25-2 (Information Assurance) and through CIO/G-6 oversight).

(3) Army Protection Program assessments (conducted in accordance with Army Directive 2011-04 (Army Protection Program)), which seek to better manage risks

[1] For example, for a systemic issue with training identified as a root cause, the Deputy Chief of Staff, G-3/5/7 and Commander, Training and Doctrine Command would be engaged through their normal business processes to support identification and implementation of a solution.

relative to the safety of Soldiers, Families, Department of the Army Civilians, infrastructure and information.

(4) Computer crime prevention surveys, which are assessments led by U.S. Army Criminal Investigation Command and directed by Army Cyber Command to prevent intrusions or other malicious network activities by identifying network vulnerabilities that are considered to be crime-conducive conditions.

(5) Communications security (COMSEC) audits and inspections conducted in accordance with AR 380-40 (Safeguarding and Controlling Communications Security Material). COMSEC audits and inspections address secure operating procedures and practices, handling and storage of COMSEC material, and routine and emergency destruction capabilities of the COMSEC account and selected operational facilities.

(6) Command Cyber Readiness Inspections, which are U.S. Cyber Command program, technical and operational inspections focusing on IA and computer network defense policies.

(7) IA Program Manager IA security reviews, which are programmatic reviews that program managers conduct annually at Army Commands, Army Service Component Commands and Direct Reporting Units in accordance with AR 25-2.

(8) Organizational Inspection Programs, which include all inspections and audits conducted by a command and its subordinate elements, as well as those inspections and audits scheduled by outside agencies in accordance with AR 1-201 (Army Inspection Policy).

(9) Information operations red team activities, which are independent, threat-based, simulated opposition force assessments that use passive, active, technical and nontechnical capabilities to expose and identify the vulnerabilities of friendly forces from an information operations threat perspective.

(10) The Inspector General Agency's IA Inspection Program. In accordance with AR 20-1 (Inspector General Activities and Procedures), the Agency carries out oversight inspections of organizational IA programs at Army Commands, Army Service Component Commands, Direct Reporting Units, the Army National Guard and U.S. Army Reserve, as well as directed systemic inspections to determine the effectiveness of such programs.

c. The proponents of these inspection and assessment programs will share information with other program proponents as needed to more effectively and efficiently manage risk across the Army. Program proponents will support the development of a consolidated IA inspection and assessment checklist, which will enable data mapping between programs, standardize expected outcomes and facilitate implementation of initial capabilities for remote assessments and continuous monitoring.

7. In the next step of the process, the proponents of inspection and assessment programs will identify systemic vulnerabilities that would seriously affect the Army if they were exploited. The proponents should inform the CIO/G-6 of any systemic vulnerabilities when identified. At a minimum, they will provide information quarterly to the CIO/G-6.

8. The IA CoP is responsible for conducting IA risk analysis and assessments of the Army's IA posture to identify and remediate vulnerabilities to real-world threats. The IA CoP will assess the likelihood and effects of exploiting a vulnerability. Recommended COAs for remediating vulnerabilities will address people, processes, technology and cost-effectiveness. Although the systemic vulnerabilities will be prioritized for resolution, a COA can and should, if possible, resolve more than one vulnerability. Specifically, the IA CoP will:

a. identify programs with IA-related data and facilitate reciprocity among programs.

b. compile and prioritize systemic vulnerabilities according to risk evaluation criteria established by the IA CoP.

(1) Army Cyber Command will provide expertise and support to assess operational capabilities and evaluate vulnerabilities for the likelihood of exploitation and operational effect.

(2) U.S. Army Network Enterprise Technology Command will provide expertise and support, and conduct inspections of Army networks to assess IA compliance.

c. identify the root causes of systemic vulnerabilities. U.S. Army Inspector General Agency will provide expertise and support in the identification of root causes.

d. develop recommended COAs to remediate vulnerabilities and present the recommended COAs to the appropriate business process owner(s) for decision.

e. oversee implementation of the selected COA(s). Appropriate business process owner(s) will make sure the IA CoP is kept current on the progress of COA implementation.

f. evaluate the effectiveness of the COA. Proponents of inspection and assessments programs will conduct targeted analysis of inspection and assessment results to support evaluation of the effectiveness of the COA.

9. References:

a. DoD Instruction 8510.01 (DoD Information Assurance Certification and Accreditation Process (DIACAP)), 28 November 2007.

b. Army Directive 2011-04 (Army Protection Program), 31 January 2011.

c. AR 20-1 (Inspector General Activities and Procedures), 29 November 2010, Rapid Action Revision Issued 3 July 2012.

d. AR 25-2 (Information Assurance), 24 October 2007, Rapid Action Revision Issued 23 March 2009.

e. AR 1-201 (Army Inspection Policy), 4 April 2008.

f. AR 380-40 (Safeguarding and Controlling Communications Security Material), 9 July 2012, Rapid Action Revision Issued 24 April 2013 (available only from Army Knowledge Online).

g. AR 380-53 (Communications Security Monitoring), 23 December 2011, Rapid Action Revision Issued 17 January 2013.