USAREC Regulation 25–2

Information Management

USAREC Cybersecurity

Headquarters
United States Army Recruiting Command
Fort Knox, Kentucky 40121-2725
30 November 2017

UNCLASSIFIED

SUMMARY of CHANGE

USAREC Reg 25-2

USAREC Cybersecurity

This revision (Administrative), dated 30 November 2017—

- Added Appendix C.
- Added User Device Checklist.
- Deleted old Chaper 2-4, added new Public Affairs Officer (PAO) section as Chap 2-4 a. through d.
- Changes to Chap 2-11 (l.) through. (v.)
- .Delete 2-12 g., change 2-12 to 2-13 Privileged Users
- added 2-13 j. and o.
- change 2-13 p. (1) (2) re-written.
- Added 4-2 C.(6).
- Added Appendix C workgroup Statement.
- Added Appendix D. USAREC Guide to Digital Ethics and Protecting Personally Identifiable Information.

Headquarters
United States Army Recruiting Command
1307 3rd Avenue
Fort Knox, Kentucky 40121-2726
Date: 1 November 2017

*** USAREC Regulation 25-2**

Effective 30 November 2017

Information Management

USAREC Cybersecurity

FOR THE COMMANDER:

ISAAC JOHNSON
COL, GS
Chief of Staff

Official:

Ronnie L. Creech
Assistant Chief of Staff, CIO/G6

History. This is a new publication effective date is 30 November 2017.

Summary. This regulation establishes the U.S. Army Recruiting Command Cybersecurity Program and sets for the mission, responsibilities and Office of Management and Budget (OMB), Committee on National Security Systems (CNSS), and Department of Defense (DOD) issuances for protecting and safeguarding Army Information Technology (IT), to include the Army-managed portion of the DOD information network (DODIN), (hereafter referred to as IT) and information in electronic format (hereafter referred to as information). Information technology includes IT infrastructure, services, and applications, used directly by the Army or for the Army by legal agreements or other binding contracts. Platform IT (PIT) and PIT systems are forms of IT and are not called out separately in this regulation.

Applicability. This regulation applies to all elements of the United States Army Recruiting Command (USAREC), all authorized users and privileged users unless otherwise stated. It applies to all USAREC Information Technology (IT) and information in electronic format at all classification levels.

Proponent and exception authority. The proponent of this regulation is USAREC Chief Information Security Officer (CISO) under guidance of USAREC Chief Information Officer (CIO). The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and risk. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. The request must include formal review by the activity's senior legal officer and endorsement by the authorizing official. Refer to Army Regulation (AR) 25–30 for specific guidance.

Supplementation. Supplementation of this regulation is prohibited without prior approval from the Chief Information Officer/G6 (RCIO), 1307 3rd Ave., Fort Knox, KY 40121.

Relation to USAREC Reg 10-1. This publication establishes policies and procedures regarding Information Management: Cybersecurity Program according to UR 10-1 para 3-16.

Suggested improvements. The proponent agency of this regulation is the USAREC Chief Information Security Officer, 1307 3rd Ave., Ft Knox, KY 40121. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ USAREC (RCIO-OPP), Fort Knox, KY 40121-2726.

Distribution. This publication is available in electronic media only and is intended for USAREC command levels.

Army internal control process. This regulation contains internal control provisions in accordance with AR 25-1, AR 25-2 and AR 11-2 and identifies key internal controls that must be evaluated (see appendix B).

*This is a revised (Adimistrative) USAREC Reg 25-2 (V2) which supersedes the UR 25-2 (1) with the same date.

Contents (Listed by paragraph and page)

Chapter 1
Introduction
Purpose •1-1, *page1*
References and forms • 1-2, *page1*
Explanation of abbreviations and terms • 1-3, *page1*
Responsibilities •1-4, *page1*
Statutory authority •1-5, *page1*
Precedence •1-6, *page1*

Chapter 2
Responsibilities
Principal Officials, Headquarters, US Army Recruiting Command; and Senior Leaders of Command and Units • 2-1, *page 2*
USAREC Chief Information Officer (CIO) • 2-2, *page 4*
The Inspector General • 2-3, *page 5*
ACofS, G-1• 2-4, *page 5*
ACofS, G-8 • 2-7, *page 6*
All personnel • 2-8, *page 6*
USAREC Chief Information Security Officer (CISO) •2-9., *page 7*
Commander, Leaders at all levels • 2-10, *page 8*
Authorized users • 2-11, *page 9*
Privileged users • 2-12, *page 10*

Chapter 3.
The USAREC Cybersecurity Program
Cybersecurity governance • 3-1, *page 12*
Governance structure at Headquarters, USAREC • 3-2., *page 12*

Chapter 4.
Implementation of the Cybersecurity Program functions and activities
Identify Function • 4-1, *page 12*
Protect Function • 4-2, *page 14*
Detect Function • 4-3, *page 17*
Response Function • 4-4, *page 19*
Recover Function • 4-5, *page 20*

Chapter 5.
User Agreements
User Responsibilities and Rules of Behavior • 5-1, *page 23*
Notice of Privacy Rights and Authorized Monitoring and Searches •.5-2, *page 23*

Chapter 6.
Acquisition/Procurement of IT Solutions
IT Products • 6-1, *page 24*
IT Services • 6-2, *page 24*
Software • 6-3, *page 24*

Chapter 7.
Reporting Requirements
Statutory Requirements for Reporting Information Required by the Federal Information Security Modernization Act of 2014 (FISMA) • 7-1, *page 25*

Privacy Impact Assessments • 7-2, *page 25*
Cybersecurity Readiness • 7-3, *page 25*
Systemic or Critical Cybersecurity Issues • 7-4, *page 25*
Cyber Events • 7-5, *page 25*

Appendixes

A. References, *page 26*
B. Internal Control Evaluation, *page 28*
C. Cyber Workgroup, *page 29*
D. USAREC Guide to Digital Ethics and protecting Personally Identifiable Information (PII), *page 33*

Glossary

Chapter 1
Introduction

1-1. Purpose

This regulation establishes policies and assigns responsibilities for the U.S. Army Recruiting Command cybersecurity program to ensure adherence to Department of the Army and Department of Defense (DoD) cybersecurity policies, processes, and standards. It integrates and coordinates with the functional elements of AR 525–2 (Army Protection Program) to safeguard Army assets. The cybersecurity program sets the conditions necessary for the Army to protect and safeguard information technology capabilities; support mission readiness and resilience; and ensure the confidentiality, integrity and availability of information in electronic format (hereafter referred to as information). It fully integrates risk management into every aspect of the Army by assigning responsibilities. It adopts the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity by establishing the five concurrent and continuous functions for managing cyber risk in a streamlined approach: Identify, Protect, Detect, Respond, and Recover, to emphasize priority of actions for protecting and safeguarding Information Technology and information.

1-2. References and forms

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities

Cybersecurity is a holistic program to manage information technology-rated security risk and to be effective it must be integrated fully into every aspect of the Command. It requires the implementation and enforcement of proper management and operational procedures by the entire organization, from commanders and senior leaders of agencies and activities providing the strategic vision and goals for the organization, to strategic planners and project and program managers, down to each individual who helps develop, implement and operate the IT that support the Army's mission and business processes. Furthermore, each individual, at every level, is responsible for procedural compliance with the proper practices and procedures for safeguarding information and IT. The responsibility for ensuring that personnel abide by these practices and procedures is inherent with Commanders and senior leaders of agencies and activities. See Chapter 2 for responsibilities.

1-5. Statutory authority

Statutory Authority is derived from Title 10, United States Code (USC), 2223; Title 40 USC 11315; and Title 44 USC Chapter 35; as well as applicable OMB Memorandums, to include reporting requirements established via the Federal Information Security Modernization Act (FISMA) of 2014, National Defense Authorization Acts, and DoD Issuances.

1-6. Precedence

This regulation is the proponent policy document for the U.S. Army Recruiting Command Cybersecurity Program for implementing Department of the Army and DoD Cybersecurity Programs. This document does not alter or supersede existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information and special access programs for intelligence as directed by Executive Order 12333, and for national security information systems as directed by Executive Order 13231, and other applicable laws and regulations. The Army will follow Director of National Intelligence (DNI), DoD and Joint Chiefs of Staff (CJCS) issuances, to include directives, instructions, security technical implementation guides (STIGs), security requirements guides (SRGs), orders and alerts. Supporting Department of the Army Pamphlets will be published to provide uniform procedures for implementing and enforcing the policies in this regulation. Compliance with this regulation and the supporting Department of the Army (DA) pamphlets is mandatory. The Army Chief Information Officer (CIO) will issue policy memorandums to provide amplifying guidance for the policies in this document when needed. Nothing in this regulation alters or supersedes the existing authorities and policies of the DoD, or the DNI regarding the protection of Sensitive Compartmented of Information as directed by Executive Order 12333. The DNI has delegated authority for all Army SCI systems to the Deputy Chief of Staff G-2. If at any time there is a conflict in this regulation with any other related DNI, DoD, or Joint issuances, the higher-level policy will take precedence. Report identified conflicts or the need for amplifying guidance on DA Form 2028. 71.

Chapter 2.
Responsibilities

Commanders and senior leaders of agencies and activities at all levels and those they appoint, to include authorizing officials for operation of IT, program managers, information system owners, application owners, IT service owners, information owners, portfolio managers, resource managers, and acquisition senior and functional services managers, are accountable for the implementation and enforcement of this regulation and will ensure individual and organization accountability within organizations and for activities under their purview.

2-1. Principal Officials, Headquarters, US Army Recruiting Command; and Senior Leaders of Command and Units.

HQ USAREC Principal Officials; Commanders, Staff, CIO and CISO leaders of agencies and activities will

a. Implement the Cybersecurity Program to ensure their personnel, processes and IT for which they have the responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition complies with this regulation and the amplifying policy guidance developed by the CIO and CISO. This includes, but is not limited to--

(1) Develop, maintain and modify IT as required to ensure uniform application of Cybersecurity policies, procedures, standards and risk management security controls in accordance with OMB, NIST, Committee of National Security Systems, DoD, Joint and Army issuances.

(2) Develop, implement and maintain the security plan for assigned IT, as described in DoDI 8510.01.

(3) Ensure that IT has been authorized to operate by the assigned Authorizing Official. Comply with all authorization decisions, including denial of authorization to operate. Enforce authorization termination dates.

(4) Transition from legacy or end-of-life Cross-Domain Solutions (CDS) to those on the Unified Cross Domain Management Office (UCDMO)-managed CDS Baseline List.

(5) Leverage the Defense Information Systems Agency (DISA)-provided Cross- Domain (CD) Services to the extent possible when a CDS is required.

(6) Provide appropriate notice of privacy rights and explain monitoring policies to all users.

(7) Require authentication per DoDI 8520.03 (Identity Authentication for Information Systems).

(8) Implement an effective vulnerability management process, which includes--

(a) Ensuring baseline configurations contain all required patches and follow applicable STIGs and SRGs at the time the baseline is established and updated with the release of new or updated Information Assurance Vulnerability Alerts (IAVAs), STIGs and SRGs.

(b) Ensure security patches are made available for new vulnerabilities and applied in accordance with the suspense dates or sooner if possible, in accordance with operational directives.

(c) Employ an automated patching process when practical in order to minimize manpower requirements and system downtime.

(d) Provide authorized personnel the access necessary to conduct required technical compliance assessments, to include vulnerability scans.

(9) Provide for vulnerability mitigation and incident response and reporting capabilities in order to--

(a) Comply in a timely and efficient manner with DoD and Army cybersecurity directives, guidance and alerts for implementing mitigations and taking corrective action in defense of the DoD Information Network (DoDIN).

(e) Limit damage and restore effective service following an incident.

(f) Collect and retain audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under their purview, and provide this data to appropriate law enforcement (LE) or other investigating agencies.

(10) Implement security-informed configuration management and change management processes in accordance with NIST guidance and as described in DoDI 8440.01 (DoD Information Technology (IT) Service Management (ITSM)).

(11) Personnel assigned to USAREC G6 Cyber Security Division will be considered mission essential and must be available for real time Cyber reporting and executions of real time cyber reporting duties.

b. Assign the appropriate responsibility and authority to individuals within the organization as necessary to implement, manage and enforce this regulation and for all applicable roles in accordance with DoDI 8510.01, Department of Defense Directive (DoDD) 8140.01 and related DoD, CNSS and Army issuances.

(1) Appoint CISO, who will thereby appoint and oversee privileged users as required to carry out appointed functions. Ensure privileged users meet the requirements for authorized and privileged users in accordance with this regulation. Monitor privileged users to ensure they continue to meet requirements. Ensure access is revoked expeditiously when users no longer meet established requirements.

(2) CISO will ensure all cybersecurity personnel under their purview are assigned in writing manage their training and certification through the Army Training and Certification Tracking System (ATCTS) at https://atc.us.army.mil.

c. CISO will ensure that all personnel--

(1) Are appropriately cleared, trained, qualified, and authorized in accordance with applicable CNSS, DoD and Army information security, communications security (COMSEC) and cybersecurity issuances before accessing IT and continue to do so during authorized access. Ensure access is revoked expeditiously when users no longer meet those requirements.

(2) Sign a user agreement of acknowledgement (paper or electronic) prior to account activation and annually there-after that they—

(a) Have read, understood and agree to abide by the rules that describe user responsibilities and expected behavior regard to information technology usage in accordance with this regulation.

(g) Have read, understood and agree to the notice of privacy rights and consent to authorize monitoring and searches in accordance with this regulation.

(3) Create and maintain a profile in ATCTS. Ensure that users' profiles are current and correct with all applicable documentation, to include completed DD Form 2875, annually signed user agreement, applicable training certificates, and as applicable, privileged access agreements, appointment memorandums and record of certifications.

(4) Ensure that military, civilian, and contractor personnel are considered for administrative and/or judicial sanctions if they knowingly, willingly or negligently compromise, damage, or place IT or information at risk by violating the user agreement. This includes--

(5) Individuals involved with misuse of the IT or violation of prohibited activities may be subject to having access suspended for a defined period of time and/or be required to complete appropriate remedial training.

(6) Non-compliance with DoD and Army regulations pertaining to the use of IT may raise security concerns about an individual's reliability and trustworthiness for access to 165 information and IT. Conditions that call into question the willingness or ability of an individual to properly protect sensitive information and IT-

(a) Will be assessed to determine whether access will be authorized, or if already authorized, whether access will be revoked. Determinations to authorize, deny or revoke access will be recorded on DD Form 2875.

(h) Shall be reported according to USAREC Regulation 190-4.

(7) Ensure contracts hold contractors responsible for ensuring employees maintain cybersecurity discipline and perform in cybersecurity discipline and perform in compliance with this regulation as well as applicable laws, policies, procedures, standards, and other related guidance.

(8) Ensure that in the event that military, civilian, or contractor personnel knowingly, willfully, or negligently violate the policies in this regulation and place at risk DOD, Army or any other Federal Government IT, punishment options will be based on the individual's status. In a non-deployment status, contractor and civilian personnel are not subject to the Uniform Code of Military Justice and therefore punishments are limited. After the investigation is completed by USACIDC IAW 195-2, contractor personnel can be removed from the Government location (Persona non grata) and returned to their private sector organization. Investigations that reveal espionage or other related acts will be referred accordingly. As for Federal civilian employees, the punishment is similar in nature in that an administrative letter of reprimand can be issued after an investigation is completed and in the event of espionage, the results of the investigation will be referred to the proper authorities for further action. With regards to military personnel subject to the UCMJ, punishment can be both Administrative in nature such as an Administrative Letter of Reprimand or it can fall under Non-judicial Punishment (NJP) with varying levels of punishments. Should the investigation warrant, military personnel will receive judicial punishment under the Courts-Martial options contained within the UCMJ. With regards to deployment of civilian personnel, DoDD 1404.10 provides for "the involuntary assignment of civilian employees to Emergency Essential (E-E) positions as may be necessary to meet the exigencies of the circumstances and when unforeseen contingencies prevent prior identification of those positions as being E-E". Army policy is to normally deploy civilian employees who either have agreed to accept E-E positions or who are volunteers. With regards to disciplinary actions, civilians are subject to UCMJ only if Congress declares war and are subject to normal administrative disciplinary action. Deployed contractor personnel fall under the UCMJ as a result of the enactment of the John Warner National Defense Authorization Act for Fiscal Year 2007 (2007 NDAA), which applies to contractors during a declared war or contingency operation.

d. Build capabilities to support cybersecurity objectives that are shared with mission partners, and ensure they are consistent with guidance contained in DoD 8000.01 and governed through integrated decision structures and processes described in DoDI 8500.01.

e. Identify and allocate resources required to implement DoDI 8510.01 as part of the Defense planning, programming, budgeting, and execution process.

f. Incorporate Cybersecurity risk assessments and decisions, in accordance with DoDI 8510.01, into Army mission and business risk management processes.

g. Ensure consistent development and implementation of Cybersecurity requirements into plans and procedures across their areas of responsibility.

h. Maintain ongoing awareness of cybersecurity threats and vulnerabilities to support risk management decisions. Ensure real-world threat data and analysis informs risk decisions. Consider shared risks. Take no unnecessary risk, but do not be risk adverse.

i. Integrate security early and throughout the IT development lifecycle, capital planning, investment control, portfolio management and enterprise architecture processes in accordance with the DoD Cybersecurity Architecture and other applicable DoD and Army issuances.

j. Integrate security standards into acquisition planning and contract administration. Ensure that contracts and other agreements include specific requirements to provide cybersecurity for information and the IT used to process that information in accordance with DoDI 8500.01 and DoDI 8510.01. Document baseline cybersecurity requirements as a condition of contract award for acquisitions utilizing IT.

k. Ensure that incident response and reporting programs are followed, and personnel are aware of, and held accountable for, daily practices that protect against suspected intrusions, unauthorized activity, suspected attacks, and other anomalous activity. Report suspected or confirmed incidents in accordance with Army regulations relevant to the specific incident, Army Cyber Command (ARCYBER) or supporting computer network defense service provider's published procedures, and formal internal policies and procedures.

l. Ensure that maintenance and disposal of information on IT complies with the provisions of DoDD 5015.2 (DoD Records Management Program) and AR 25-400-2 (The Army Records Information Management System).

m. Comply with the specific policies developed by the Chief Information Officer (CIO) for TRADOC and Army cybersecurity program in accordance with statutory requirements outlined in the FISMA of 2014.

n. For all assigned IT, comply with Authorizing Officials' decisions.

o. Comply in a timely and efficient manner with DoD, Army cybersecurity issuances and TRADOC for implementing mitigations and taking corrective action in defense of the DoD information network.

p. Include assessments of current cyber risk to capabilities and missions.

q. Conduct DoDIN operations and Defensive Cyberspace Operations - Internal Defense Measures (DCO-IDM) in accordance with directives issued by U.S Army Cyber Command.

2-2. USAREC Chief Information Officer (CIO)

In addition to the responsibilities in paragraph 2-1, the Army CIO will--

a. Establish and supervise USAREC's Army cybersecurity program and issue policies and guidance for Army cybersecurity activities to support DODIN operation as described in DODI 8530.01.

b. Issue policies and guidance for USAREC Chief Information Security Officer (CISO) Army cybersecurity activities to support DoDIN operations as described in DoDI 8530.01, Cybersecurity Activities to Support DoD Information Network Operations.

c. Set the strategic direction, policy, and verify enterprise resources are used effectively for Army-wide activities to design, build, configure, secure, operate, maintain, modernize and sustain the Army-managed portion of the DoD information network and to protect and defend IT by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

d. Promulgate policies and guidance to ensure that all IT complies with applicable law, national, federal, and DOD issuances, to include, National Security Agency (NSA) issuances, National Institute of Standards and Technology (NIST) standards, DOD Security Technical Implementation Guides (STIGs), and DOD Security Requirement Guides (SRG), with exceptions documented and approved by the responsible Authorizing Official.

e. Include USARECs cybersecurity architecture for management of the Enterprise portfolio as described in DoDD 8115.01 (Information Technology Portfolio Management).

f. Validate that IT investments comply with DoDI 8500.01, to include leveraging DoD-wide cybersecurity solutions to the extent practical; DoDI 8530.01; and are consistent with DoD and Army cybersecurity architecture.

g. In conjunction with TRADOC and HRC, ensure in-depth cybersecurity orientation, training, certification and awareness programs are developed and made available to all Army personnel.

h. Serve as the Authorizing Official for all IT within the purview of this regulation and ensure it is authorized in accordance with the DoDI 8510.01.

i. Ensure an appointment of the USAREC Chief Information Security Officer (CISO) via the Cyber Security Chair.

j. CISO is assigned as the Code Signing Authorizing Official.

k. Advise USAREC mission area lead to ensure that cybersecurity requirements are addressed for all IT.

l. Ensure that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing Army- owned or controlled IT.

m. Issue policy and guidance to ensure that cybersecurity solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities or access to or use of information and data by individuals with disabilities in accordance with law and DoD issuances.

n. Ensure that cybersecurity requirements are addressed and visible in all capability portfolios, properly addressed during IT development within the attributes of the non-kinetic (cyber) piece of the Systems Survivability (SS) key performance parameter (KPP), technical architectures, IT lifecycle management processes, and investment programs incorporating IT.

o. Ensure the System of Systems Network Vulnerability Assessments (SoS NVA) is integrated into the Army Interoperability Certification (AIC) program.

p. Coordinate with the Inspector General to identify root causes and solutions for systemic and critical cybersecurity issues reported to the CISO.

q. Issue and annually review the requirements that govern the appropriate use of Army IT that will be included in all Army IT user agreements.

r. Validate whether PPP cybersecurity strategy annexes comply with DoDI 487 8510.01 and DoDI 5000.02.

s. Provide regulatory and policy direction and oversight for the Authority to Operate (ATO) and Authority to Connect (ATC) processes.

2-3. The Inspector General

In addition to the responsibilities in paragraph 2-1, the Inspector General will--

a. Conduct an annual independent evaluation to determine the effectiveness of the Army Cybersecurity Program and practices, using 44 USC 354 as a guideline.

b. Leverage the cybersecurity mission essential talk list to identify systemic readiness issues and report the root causes of such at least annually.

c. Coordinate with the USAREC CIO and USAREC CISO to identify root causes in support of identifying solutions systemic and critical cybersecurity issues reported.

d. PAO is responsible to establish PAOs at every level determined necessary to support the mission. Copy of PAO orders will be provided to USAREC CISO.

2-4. Public Affairs Officer (PAO)

a. The PAO will provide policies, procedures, and format conventions for Web sites, Social Media and other public content.

b. PAO will ensure with G7/9 that any command maintaining publicly available accessible Web sites must register Web, Social Media and other public content to https://span.usarec.army.mil/sites/HQ/G7-G9/Lists/Social_Media/AllItems.aspx. PAO is responsible to approve all WEB content.

c. PAO will ensure feedback method is established to review all public facing WEB contact. All sites will be regisitered and provided to USAREC CISO.

2-5. ACofS, G-1

In addition to the responsibilities in paragraph 2-1, the DCS, G-1 will --

a. Assign a position designation (PD) for personnel occupying cybersecurity positions using the criteria found in DoD 5200.2-R and DoDI 1400.25 Vol. 731 and document in the Defense Civilian Personnel Data System (DCPDS).

b. Ensure the PD includes the associated suitability and fitness requirements in accordance with DoD policies, procedures, standards, and other guidance as described in DoDI 1400.25, Vol 731.

2-6. ACofS, G-6 The Office of the G-6 will—

In addition to the responsibilities in paragraph 2-1, the office of the G-6 will-

a. Promote and facilitate the Army cybersecurity program and related activities to support DODIN operations and Defensive Cyber Operations (DCO) as described in DODI 8530.01.

b. Provide management oversight of cybersecurity activities to support DODIN operations and DCO internal defensive measures as described in DoDO 8530.01.

c. Appoint via the Cyber Chair a CISO to manage the resources for USAREC cybersecurity programs.

d. Ensure that cybersecurity inspections and compliance oversight activities are accomplished in coordination with AR 525-2 and that the cybersecurity trend information is shared with key stakeholders.

2-7. ACofS, G-7/9 The Office of the G-7/9 will—
Because the Internet is a public forum, the G7/9 is responsible for USAREC public affairs officer (PAO), and other appropriate designee(s) (for example, Brigade or Battalion PAOs may be appointed by the Deputy Chief of Staff G-7/9 and will furnished a copy of appointment orders to USAREC CISO, PAOs will be considered the authorized reviewer) will ensure public web including Social Media sites have been properly cleared information posted in areas accessible to all account types.

a. Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the WWW. The appointed reviewer(s) will conduct routine reviews of Web sites, including Social media on a quarterly basis to ensure that each site is in compliance with the policies herein and that the content remains relevant and appropriate. The minimum review will include all of the Web site management. Information contained on publicly accessible Web sites including Social Media is subject to the policies and clearance procedures prescribed in AR 360–1, chapter 5, for the release of information to the public. In addition, organizations using the WWW will not make the following types of information available on publicly accessible Web sites:

(1) Classified and restricted or limited distribution information.

(2) FOUO information.

(3) Unclassified information that requires special handling (for example, encrypt for Transmission only Limited Distribution, and scientific and technical information protected under the Technology Transfer Laws).

(4) Sensitive information such as proprietary information, pre-decisional documents, and information that must be protected under legal conditions such as the Privacy Act.

(5) FOIA-exempt information. Lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization, or office in the DA are prohibited on the WWW. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties—such as general officers and senior executives, PAOs, or other personnel designated as official command spokespersons is permitted.

(6) Documents or information protected by a copyright.

(7) Draft Publications.

b. The Army G-7/9 will provide policies, procedures, and format conventions for Web sites, Social Media and other public content.

c. G-7/9 will ensure the any command maintaining publicly accessible Web sites must register Web, Social Media and other public content to https://span.usarec.army.mil/sites/HQ/G7-G9/Lists/Social_Media/AllItems.aspx. G-7/9 will ensure contact is updated and PAO approved.

2-8. ACofS, G-8

In addition to the responsibilities in paragraph 2-1, the DCS, G-8 will provide independent assessment for the development, integration, and defense of programming to support USARECs cyber investments.

2-9. All personnel

Every individual at each level is responsible for procedural compliance with the proper practices and procedures for safeguarding information and IT. Military and civilian personnel will be considered for administrative or judicial sanctions if they knowingly, willfully, or negligently violate the acceptable use policy or otherwise compromise, damage, or place at risk DoD or Army information or IT by not following this regulation and the applicable DoD and Army issuances. Contractor personnel need to be informed that there may be consequences if they disobey policy.

Personnel at all levels must ensure each user and subordinates are aware of their responsibilities to prevent the loss or theft of government owned/leased IT devices. These devices are known targets of theft because of their portability, cost and likelihood to contain sensitive information. This policy provides guidance on the security of IT devices as well as the reporting of loss of these devices and the correlating exposure of compromised PII. In addition to Government proprietary information, IT devices often contain PII and FOUO data. Unauthorized access creates potential risks to USAREC and Army operations ranging from unauthorized disclosure of sensitive personal and operational information to intrusions and data gathering within our network. The loss of these devices may adversely impact operations requirements and mission accomplishment. In the wrong hands, this information could damage the reputations of USAREC and the Army.

2-10. USAREC Chief Information Security Officer (CISO)

Direct report to USAREC CIO, the CISO will direct and coordinate the Army cybersecurity program, to include but not limited to--

a. Oversee development and dissemination of the overall cybersecurity policy for USAREC.

b. Oversee the USARECs Security Control Accessor (SCA) function to include assessment of the quality, capacity, visibility, and effectiveness of cybersecurity assessments, and directing modifications as necessary. Formally delegate the SCA role for governed information technologies as he/she deems necessary.

c. Serve as USARECs voting member in the Requirements Review Board (RRB) and Executive Requirements Review Board (ERRB).

d. Develop policy to ensure that the USAREC cybersecurity assessment process remains consistent with TRADOC and DoD policy and guidance.

e. Adjudicate and resolve process issues and concerns.

f. Establish priorities for Assess and Authorize package processing associated with command activities.

g. Develop qualification standards for the cybersecurity professionals responsible for conducting security assessments.

h. Advise and inform the principal authorizing officials (PAOs) and their representatives.

i. Oversee implementation and enforcement of DoDI 8510.01 within USAREC.

j. Establish and oversee the workforce of cybersecurity professionals.

k. Serve as the single cybersecurity coordination point for USAREC-wide 955 programs that are deploying information technologies to USAREC enclaves.

l. Coordinate with GOV to integrate cybersecurity concepts into the USAREC acquisition process.

m. Coordinate with the CIO to ensure cybersecurity testing and evaluation is integrated into the acquisition process.

n. Develop USAREC-specific assignment values, implementation guidance, and validation procedures.

o. CISO will be appointed via the USAREC Deputy Commanding General (DCG), CISO will have direct access to DCG for matters of Cyber Security that may put the command at additional risk.

p. CISO holds veto authority for all Information Technology projects, testing and evaluation.

q. CISO will create and maintain USARECs Cyber Workgroup and will provide cyber updates to the Cyber Chair as necessary to support the mission.

r. CISO will establish operations that support real time reporting for Cyber readiness within USAREC. This may include extended or subject to recall duty hours and may require travel as necessary to support the mission.

s. CISO will coordinate with leadership as necessary to ensure all active duty personnel are exempted from duty rosters, in support of real time cyber reporting

t. CIO or CISO are the only authorized officials for unit Information Assurance Technical (IAT) or Information Assurance Managers (IAM), individual technical orders are to support DOD 8570 certification requirements and the Army Training and Certification Tracking System (ATCTS).

u. CISO will select, train and appoint the Command Cyber Inspection Team (CCIT). CCIT will support physical security responsibility of the Command Cyber Readiness Inspection (CCRI). CCIT will be identified through Cyber Security Identification Card and appropriate Cyber Security Badge, issued via the CISO. CCIT has full authority to make on the spot corrections and minimize any cyber/network threats.

v. CISO during Continuity of Operations (COOP), the CISO is considered MEF A-D ERG workforce and will designate as needed to support COOP ERG workforce mission operations. CISO and designated assigned Cyber representative will ensure that Cyber operations are available and operational in real time. Contracted workforce will not be affected and will take all directions by the COR. CISO will ensure mission essential ERG workforce is equipped with appropriate tool kit to ensure continuous operations.

w. CISO will in event to command COOP plan support will identify essential resources, files, databases, security of telecommunications equipment (telephone units, telephone equipment, laptops. tablets, printers and network devices) and provide management of application of these at each ERF site. CISO will develop a plan to resources and support approximately 50 USAREC HQ staff personnel with automation and communications equipment during an LOR 3 incident. CISO will establish reliable process and procedures to acquire and sustain IT resources necessary to continue MEFs during a long-term event (up to 30 days). CISO will manage the Commanding General’s secure phone; CISO and staff will ensure his/her telework agreement is updated and ready to execute.

x. CISO has approval authority for non-government issued Information Technology equipment, approval by CISO must be in writing and will provided any risk mitigation. Information systems approved by CISO are subject to inspection for any data or technical risk.

y. CISO has full approval or disapproval authority for the USAREC Cyber area of operation (AO). Supporting the Recruiting mission and unique network environment requires hardware, software or other devices to securely support the .COM/.EDU domain(s), including any items that may be considered inappropriate for the Cyber Area. Cyber area will be kept organized, area will remain professional and welcoming for any individual within the command that requires support.

z. Traditional takedown process will be utilized when possible (see UP 25-1-1), however CISO has authority(s) to mitigate risk within Social Media and Websites (Domain) by initiating an immediate site takedown.

2-11. Commander, Leaders at all levels

a. Leader's will- report theft, loss or other circumstances where Information Technology devices are outside government control, immediately to the CISO via email or telephone. In cases where the CISO is unable to be contacted, the Command Operations Center will receive and log the incident and will email the CISO.

b. Report in real time to the CISO at usarmy.knox.usarec.mbx.hq-g6-ia-office@mail.mil any loss or suspected loss of Personally Identifiable Information (PII), or Sensitive Personal Information (SPI), defined by US privacy law and information security, as information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Serious Incident Report (SIR) IAW 190-4 can be submitted later as needed, however leaders have a responsibility to report immediately

c. Loss or theft of IT devices (computing devices and other devices with storage capabilities) including but not limited to: laptop computers, tablets, smartphones, USB flash drives, external hard disk drives, multi-function printers, etc. must be reported via Serious Incident Reporting procedures outlined in UR 190-4.

d. Leaders must ensure that they notify affected individuals within 10 working days when personal information was stored on that device. USAREC Cyber Security Division will supply units with PII information. This does not apply if it can be reasonably determined that the information contained on the device was not compromised, (i.e., destruction by fire, flood, etc.).

e. Physical Security of Devices.

(1) Leaders and supervisors are responsible for evaluating the risk and vulnerabilities of loss or theft and must take all reasonable measures necessary to ensure adequate safeguards are in place for all sensitive information and IT equipment.

(2) Unassigned IT devices (including temporary personnel absences due to illness, leave, school, etc.), will be secured in a locked metal filing cabinet or other lockable container out of plain view or in a secure room with limited, controlled access. Assigned IT devices will be secured in a locked cabinet, locked office, or other secure location.

(3) Liability for the loss or theft of IT devices shall be determined IAW this policy and AR 735-5. Failure to follow this policy or other guidance for security of IT devices will constitute negligence and subject the violator to personal liability.

(4) The USAREC G-4 will disallow any property book adjustments for lost/stolen IT devices until after validation that an SIR was generated and submitted through command channels.

(5) Accountability of IT devices will be included with cyclic inventory procedures as required by AR 735-5.

f. When travelling with an IT device outside the regular place of duty:

(1) Do not leave an IT device unattended in a POV or GOV. This prohibition applies even if the vehicle is locked, the device is in the trunk, or the device is secured by an approved locking device such as a cable lock;

(2) Personnel will carry their IT devices on their person or otherwise maintain positive visual or physical control of the IT devices while traveling. If the device's carrying case is too large to be carried aboard aircraft, personnel are required to remove the IT device from its case and hand carry it onto the aircraft.

(3) Personnel must make every effort to not leave IT devices unattended in hotel rooms.

(4) Personnel must make every effort to secure IT devices when at their personal residence.

g. Reporting/Recovery of It Device Theft, Loss, or Compromise of PII Data.

(1) All losses, thefts of IT devices, and compromises of PII will be immediately reported through command channels as directed by UR 190-4.

(2) The initiator's commander will notify the affected individuals of compromised PII within 10 calendar days of the event. Failure to notify affected individuals within 10 calendar days will require the USAREC CG to inform the Deputy Secretary of Defense for the reasons why notification was not provided. Examples of memorandums and decision tables are available on the G6 SharePoint: http://span.usarec.army.mil/sites/HQ/G6/IA/.

(3) The COC will notify USAREC CISO of the reported loss, theft, or compromise, follow up and final reports of loss, theft, or compromise of any IT equipment or PII within one hour of incident notification. COC will report to US-CERT. CISO will coordinate with USAREC G6 Records or Privacy Act Manager for notification to TRADOC using DA Form 2959 of all incidents involving PII within one hour of discovering the incident, and will provide a courtesy copy to USAREC's PAO and COC. USAREC G6 Records or Privacy Act Manager will provide COC, PAO, IAPM, TRADOC and US-CERT with follow up and final PII reports. PII reporting process is available on the G6 SharePoint.

h. When sending PII/PHI or other sensitive FOUO information, users will ensure to digitally encrypt the email, IAW AR 25-1. CISO will notify user and user's chain of command of the email encryption violation. USAREC CISO will establish standardized actions appropriate to the violation(s) and provide recommendation(s) to the commander for consideration. Leader or user must provide documented proof of corrective action within forty eight hours (2 duty days) to USAREC Information Assurance / Cyber Division or user account will be disabled by CISO.

i. Will take appropriate action IAW 600-20 for any Cyber violations. Leaders will ensure that USAREC Cyber receives finalized action, no details will be provided, just that the leader took appropriate action IAW 600-20.

j. Will ensure that process defined in USAREC Pam 25-1-1 are adhered to, variations are authorized in writing by the CIO or CISO.

k. Will ensure that all users register each device or service within the Headquarters Support System (HSS) database.

l. Will ensure that each user has the latest Enterprise Mobility Management tools installed, operating and reporting as designed. To be compliant with cyber security policy, mobile devices must meet the following criteria:

(1) Both the Device Management and Identity authentication applications are properly installed and configured on the mobile device. Personnel will not issue, take possession of, or utilize a government furnished mobile device without current device management and identity authentication tools completely installed.

(2) Mobile device is up-to-date with the latest approved operating system (OS) and security patches. The device management tool will inform the user when to update. Do not allow the device to update when the vendor or manufacturer releases an update unless explicitly provided that guidance from USAREC G6. For information on the latest approved OS, you may visit the device management home web site if available.

m. Will ensure that devices with zero usage (e.g., Devices that are not used at least once every 30 days) are reviewed. These devices pose a cyber security threat and will be temporarily suspended. Users not utilizing government furnished equipment will be reported to the USAREC CISO. Commanders will investigate as appropriate.

n. Ensure each user completes the appropriate Information Assurance, Cyber training and Acceptable Use Program (AUP) as required.

o. Will ensure funds appropriated for Information Technology are utilized and processed in accordance with USAREC Regulation 25-1.

p. Will ensure ADPE funds and acquisition of Information Technology equipment is properly accounted for.(AR 25-1,para 1.6a)

q. Will ensure ADPE funds tracking is done IAW AR 25-1, para 1-6a and AR 25-400-2.

r. Ensure all Technology acquisitions are evaluated in terms of direct support and compatibility with Army Enterprises solutions, mandates and process, including their corresponding information requirements, (AR 25-1, para 1-6b(2)).

s. Ensure acquisitions for Technology solutions are processed IAW 25-1, para 2-3a.

t. Ensure unit is utilizing the decision baseline outlined in USAREC Regulation 25-1 for acquisition of technology equipment. (UR 25-1. Para 2-4)

u. Ensure use of USAREC Basis of Issue Plan as part of their validation process for technology service request. (UR25-1, para 2-3a)

v. Ensure use of DA Form 3953 for requesting technology supplies and service. (UR 25-1, para 2-3a)

2-12. Authorized users

Authorized users will-

a. Meet DOD cybersecurity awareness requirements in accordance with DOD 8570.01-M and establish an Army Training and Certification Tracking System (ATCTS) account prior to gaining network access and compete and record awareness training annually.

b. Use IT only for official or authorized purposes.

c. Ensure classified and unclassified sensitive information/CUI is only accessed, stored and processed on IT is formally and explicitly authorized for the classification level, caveats, and sensitivity of the information IAW 5200.01 and 5230.11.

d. Immediately report all Cybersecurity-related events (for example, unauthorized disclosure) and potential threats and vulnerabilities (for example, insider threat) to USAREC Cyber Division (usarec.knox.usarec.mbx.hq-g6- ia-office@mail.mil, Local S6 or Leadership.

e. Authenticators for accessing IT and information--such as passwords, PINs, Common Access Cards, and other smartcards— are sensitive components and will be safeguarded appropriately to prevent their loss or compromise. Report the loss to the appropriate CAC Issuance Office IAW AR 600-8-14.

f. Protect terminals, workstations, other input or output devices and resident data from unauthorized access.

g. Processes will be followed per USAREC Pam 25-1-1.

h. Adhere to policies and procedures governing the secure operation and authorized use of IT, including operations security. All users are responsible for ensuring that mobile devices are compliant with cyber security policy and adhering to the policies and procedures that govern the secure operation and authorized use of IT.

i. Meet the security clearance requirements in AR 380-67 for the classification level of the information processed by the IT system they are accessing.

j. Foreign exchange personnel and representatives of foreign nations, coalitions, or international organizations may be authorized access to IT and information in accordance with national, DoD, and Army issuances and IT security authorizations.

2-13. Privileged users

Privileged users are individuals who are authorized to perform security-relevant functions that ordinary users are not authorized to perform. Only those users who require privileged/elevated access to carry out their assigned functions are eligible to be a privileged user. All active Army, Army National Guard/Army National Guard of the United States and the Army Reserve will follow all policies and responsibilities regarding privileged users. All active Army, Army National Guard/Army National Guard of the United States and the U.S. Army Reserve will follow all policies and responsibilities regarding privileged users. In addition to the requirements in para 2-26, will--

a. Obtain within six months of being appointed as a privileged user and maintain there after the appropriate DODD 8140.01 and DOD 8570.01-M 831 certifications.

b. Hold an active security clearance that commensurate with the classification level of the information processed by the IT they are accessing.

c. Review, complete, and sign (physically or digitally) a Privileged Access Agreement (PAA) update in ATCTS (http://atc.us.army.mil) prior to using privileged access.

d. Review, complete, and sign (physically or digitally) a Non-Disclosure Agreement (NDA) and update in ATCTS prior to using privileged access.

e. Configure and operate IT within the authorities vested in them, in accordance with the applicable DoD and Army issuances.

f. Require use of PKI or other multifactor authentication to implement applicable Cybersecurity controls, per DODI 8510.01.

g. Only the CISO appointed will oversee command/organization user accounts for cybersecurity program will authorize or deny each request then forward to the service provider for consideration. They are primary cybersecurity duties within Army organizations and within the RMF process.

h. Service provider will authorize or deny the granting of privileged/elevated access for enterprise managed system user accounts.

i. Service provider will revoke privileged/elevated access when--

(1) User account documentation is not fully compliant.

(2) Positions and/or functions no longer require such access.

(3) Notified by the Command or Army activity that such access is no longer required.

j. Service provider enforce all privileged user policies.

k. Service provider will authorize appointment letter guidelines found in subsequent DA Pamphlets.

l. Use PKI credentials issued through the Army PKI Registration Authority (Army RA) for all privileged user access to NIPRNET, SIPRNET, DREN and SDREN systems. Alternative multi-factor authentication technology may be used only when authorized by the Army CIO.

m. Commands and Service Providers will monitor all personnel with privileged access to Army IT and information.

n. Revalidate all users with privileged/elevated access and routinely thereafter.

o. Conduct DoDIN operations and Defensive Cyberspace Operations - Internal Defense Measures (DCO-IDM) in accordance with directives issued by ARCYBER.

p. Access to data, systems and network resources that are determined privileged by the Chief Information Security Officer (CISO) may require additional training, certification or agreement on the part of the user.

(1) Access to REQUEST and the ability to enter into a contract agreement for Officer and Enlisted US Army Soldiers both Active and Reserve, user must be US Army ASI V7 (Guidance Counselor) qualified. Exceptions may be granted if the user is training for ASI V7 and is scheduled for ASI V7 qualification within six (6) months of assignment. ASI V7 is required to remain qualified and be in a position that requires a REQUEST account. Exceptions will be sent to USAREC CISO. USAREC G3 and USAREC CISO must concur for exception approval. USAREC CISO has final exception approval documentation and approval for privileged access.

(2) Access to REQUEST without the ability to enter into contract agreement, supporting reports, data mining, process improvement, investigations, etc. will not require ASI V7. Questions regarding access will be directed the USAREC CISO.

Chapter 3.
The USAREC Cybersecurity Program

In support of a holistic Cybersecurity program that is integrated fully into every aspect of USAREC, USAREC is leveraging the functions and activities from the NIST Framework for Improving Critical Infrastructure Cybersecurity (see chapter 4). When considered together, these functions provide a high-level, strategic view of the Commands and Army's cybersecurity risk management lifecycle and support mission readiness and resiliency. These functions do not replace, but support Cyber Operations functions outlined in the applicable Joint Publication issuances. USAREC cybersecurity program synchronizes and standardizes cybersecurity requirements for safeguarding IT and information to support the execution of critical Army missions and essential functions. USAREC must-

a. Incorporate cyber risk management principles and best practices into organization-wide strategic planning considerations, core missions and business processes, and supporting organizational IT.

b. Integrate cybersecurity requirements into system development lifecycle processes.

c. Establish practical and meaningful boundaries for organizational information systems to identify what the organization is responsible for protecting, to include those protections under its direct control and management or within its scope of responsibilities and include people, processes and information technologies that are part of the systems supporting the organization's missions and business processes.

d. Plan for the following when managing cyber risks to minimize the impact on DoD and Army missions and business operations--

(1) Operational resilience--

(a) Ensure information resources are trustworthy by meeting TSN requirements and best practices in accordance with DoDI 5200.44.

(b) Missions are prepared for information resources degradation or loss by performing developmental T&E of cybersecurity.

(c) Ensure network operations have the means to prevail in the face of adverse events by establishing proactive protective internal defensive measures.

(2) Interoperability-- Ensure the ability of IT to communicate with other Army and DoD IT as required.

(3) Cyberspace defense will be employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on DoD information networks. Cyberspace defense information will be shared with all appropriately cleared and authorized personnel in support of DoD enterprise-wide situational awareness.

(4) Performance-- Manage mission outcomes based on strategic goals and objectives.

(5) DoD, Army and USAREC information-- Implement policies and procedures required by DOD/Army in operational environments to minimize risk.

(6) Identity assurance-- Verify credentials to ensure users are authorized and in compliance with DoD standards.

(7) Workforce-- Follow DoD guidelines to manage the work function of cybersecurity objectives.

(8) Safeguard information using required levels of protection processes to support Cybersecurity objectives in line with Defense Support to Civilian Agencies and Partner Assisted missions.

(9) Culture of accountability-- Work to protect Army-wide responsibilities by aligning mission goals and standards, in accordance with cybersecurity guidelines.

(10) Shared risk responsibility-- Manage responsibilities in a cohesive operational environment to mitigate disruptive events.

(11) Adherence to DoD and Army architectures-- Follow DoD and Army guidelines and procedures and adhere to DoDI 8510.01.

(12) Continuous monitoring-- maintain ongoing awareness of information and IT in order to support risk-related decisions at all tiers (Army as an organization, mission/business processes and the IT itself). Utilize information readily available through the implemented security controls.

(13) Reciprocity—USAREC will utilize the Army process and will use the DoD repository, Enterprise Mission Assurance Support Service (eMass) or its successor, for sharing security authorization packages and risk assessment data with Authorizing Officials from other organizations in order to reduce redundant testing, assessing and documentation, and the associated costs in time and resources, and to support making credible, risk-based decisions regarding the acceptance and use of systems and the information that they process, store, or transmit.

3-1. Cybersecurity governance

Governance provides strategic guidance, ensures cybersecurity objectives are achieved, evaluates whether risk is managed appropriately, and verifies that enterprise resources are used effectively. Governance activities will ensure—

a. Alignment of cybersecurity objectives with mission and business strategies.

b. Understanding of the regulatory, legal, risk, environmental, and operational requirements and that these requirements inform the management of cyber risk, policy development and resource allocation.

c. Integration of cybersecurity considerations and requirements into processes involving strategy development, enterprise architecture, capital planning and IT portfolio management, budget oversight, workforce planning, training and education, service level agreements, supply chain risk management, mission partner relationships, traditional security and risk management programs, and inspections, audits and investigations.

d. USAREC risk management and compliance processes provide for the effective management of cyber risk as the strategic-, mission and business process- and IT levels in accordance with DoDI 8500.01, DoDI 8510.01, and related CNSS, NIST and DoD issuances. Baseline security controls will be developed IAW AR 25-30 and DA PAM 25-40. Published guidance will be posted on the DOD RMF KS at https://rmfks.osd.mil in the Army workspace therein.

e. USAREC cybersecurity roles and responsibilities are coordinated and aligned within Army and with mission partners.

f. CISO will be included in all IT purchases and will sign off on solution or products to meet audit requirements.

3-2. Governance structure at Headquarters, USAREC

a. The USAREC CIO is responsible for ensuring appointment of CISO that will oversee the governance of the USAREC Cybersecurity Program. The governance structure is comprised of--

1-2 USAREC Executive Review Board (ERB). The ERB provides strategic guidance and direction to the Command, related to the USAREC CIO's authority and responsibility, to take action on all matters related to Information Resources Management (IRM), cybersecurity, and IT Architecture. The CIO-EB ensures stakeholder needs and conditions are evaluated to develop balanced, enterprise-wide IRM, cybersecurity, and IT Architecture objectives.

Chapter 4.
Implementation of the Cybersecurity Program functions and activities

USAREC Cybersecurity Program is aligned to the five core functions of the NIST Cybersecurity Framework (the Framework): Identify, Protect, Detect, Respond and Recover. Leveraging the Framework positions the Army to focus on the functions and activities that will make a significant impact on the Army's ability to protect and safeguard IT and information. Furthermore, it aligns the Army to National level objectives and supports military objectives while enabling Army to make the best use of its resources. Implementing these five functions help organizations reduce and manage cyber risk. Commanders and senior leaders of agencies and activities at all levels will implement the processes necessary to carry out these functions and activities consistent with their responsibilities, missions, functions, and tasks.

4-1. Identify Function

The activities in the Identify function develop the organizational understanding to manage cyber risk to IT and information in order to safeguard mission-essential functions down to Commands' execution of operational plans, contingency plans and vital, mission-essential tasks. Understanding the mission and business context, the resources that support critical functions, and the related cyber risks enables an organization to focus and prioritize efforts, consistent with its risk management strategy and mission and business needs. DODI 8510.01 includes the method for determining risk. It also introduces several roles which work together to maintain cybersecurity for information technology. Information concerning the specific responsibilities, duties and relationships to each other are captured in this regulation and in the RMF DA PAM.

a. Assess and Manage Cyber Risk. Cyber risk is one component of the overall risk environment and will inform organizations' risk management strategies and activities. Cyber risk must be included in risk assessments and addressed appropriately in decision-making processes, to include strategic and operational planning, policy development, requirements development and validation, development of solutions, and resource allocation and execution. USAREC will follow TRADOC and Army adherence to DoDI 8510.01 policy and procedures for assessing and managing risk in accordance with CNSS and NIST issuances. IT will be registered in accordance with DoDI 8510.01 in the DoD provided registry, eMASS, or its successors. Refer to the DoD RMF KS, https://rmfks.osd.mil, and the Army Workspace on the DoD RMF KS for Army specific implementation guidance. Risk management required activities include-

(1) Identify the risks associated with vulnerabilities inherent in IT, global sourcing and distribution, and adversarial threats to the Army's use of cyberspace in employment of warfighting, intelligence, business and enterprise information environment capabilities. Risk assessments will include vulnerability assessments of ports, protocols and services and be documented and approved as part of DoDI 8510.01.

(2) Address risk as early as possible and in an integrated manner across the IT lifecycle.

(3) Management of the risk commensurate with the impact of loss of confidentiality, integrity, and availability assigned to the potentially affected information, information technology or other assets based on the missions they support.

(4) Obtain and report security risk posture status and adherence with policies, principles, standards, procedures, and methodologies. Confirm that corrective actions to address gaps within the accepted level of risk associated with IT assets are closed in accordance with plans of actions and milestones approved by the responsible Authorizing Official as well as directed timelines.

(5) Designate and categorize IT in accordance with DoDI 8510.01 (Risk Management Framework (RMF) for DoD IT).

(6) Define authorization boundaries in accordance with DoDI 8510.01.

b. Analyze mission and business environment. Include IT and cybersecurity considerations in--

(1) Mission analysis when identifying and prioritizing critical mission essential functions, other operational requirements, and critical assets to focus Army Protection Plan priorities and resources.

(2) Risk assessments to inform risk decisions.

c. Plan for resilience. Plan, develop, test, implement, evaluate, and operate IT to ensure--

(1) Information and services are available in a secure manner to authorized users whenever and whenever required according to mission needs, priorities, and changing roles and responsibilities.

(2) Operational and enterprise objectives are met.

(3) Applicable cybersecurity laws, regulations, and standards are met.

(4) Business impact analysis are conducted to identify important services to the enterprise, to map services and resources to business processes, and to identify mission dependencies. The purpose of the analyses is to--

(a) Ensure that the impact of unavailable resources is fully agreed upon, and accepted by the organization.

(b) Ensure that, for vital business functions, Service Level Agreement (SLA) availability requirements can be satisfied.

(5) Mission processes are defined with consideration for Cybersecurity and the resulting risk to organizational operations, IT assets, and users.

(6) Cybersecurity is fully integrated into system lifecycles and is a visible element of IT portfolios.

(7) Information protection needs arising from mission requirements are assessed and IT processes are applied to support them.

(8) Interoperability is achieved through compliance with DoDI 8330.01, adherence to the DOD architecture principles, and adoption of a standards-based approach by all organizations sharing an acceptable level of risk necessary to achieve mission success.

(9) All interconnections of IT are managed to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems.

(10) Contingency plans are developed, tested, reviewed, and adhered to, for all IT assets can be considered for contingency planning.

(11) Cybersecurity issues are addressed in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

(12) Analysis of all IT assets is conducted to determine criticality to the organization and to determine prioritization of mission-critical functions and dependencies.

(13) Business continuity management options are determined and a cost-effective and viable continuity strategy is chosen that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption.

d. Manage IT assets. Manage IT assets through their lifecycle to make sure they are accounted for, physically protected, and those assets that are critical to support mission and business processes are reliable and available. Required activities include--

(1) Ensure that physical devices and systems, software platforms and applications are inventoried and tracked so that only authorized devices are given access to the network, and unauthorized or unmanaged systems, devices, or software found is prevented from gaining access or execution.

(2) Identify and manage IT that enable the organization to achieve mission and business objectives.

consistent with their relative importance to those objectives and with Army strategic and operational risk decisions.

(3) Prioritize resources for protection (for example, hardware, devices, data, and software) based on their classification, criticality, and business value.

(4) Manage assets from procurement to disposal to ensure that assets are accounted for and protected, in accordance with applicable Army cybersecurity policies, standards, and architectures.

(5) Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (for example, suppliers, customers, mission partners) through the lifecycle.

(6) Require newly acquired IT products to be free of known security vulnerabilities or establish an Authorizing Official approved risk mitigation strategy to manage the risk to an acceptable level.

(7) Program for technology upgrades and continued support from a qualified Army software maintainer or vendor as necessary to ensure continued compliance with applicable laws, NIST standards, and DoD strategic and operational risk decisions. In the case of open source or custom software, a qualified DoD software sustainment organization, such as the software centers under AMC, or vetted government contractor vendor must be engaged to properly maintain the open source components. Use of open source must be approved by the Authorizing Official with purview over the system or product. Use of shareware and freeware often involve significant risks and serious legal issues and are not permitted unless a documented exception is granted by the USAREC CISO, USAREC CIO and sent through TRADCO to Army SISO for final approval.

(8) Ensure all IT products installed are supported by the vendor for security patches to address publicly known security vulnerabilities.

(9) Manage, mitigate, and monitor (as appropriate) risks associated with global sourcing and distribution, weaknesses or flaws inherent in the IT, and vulnerabilities introduced through faulty design, configuration, or use.

(10) Ensure standard mandatory notice and consent banners are displayed at logon to all IT in accordance with applicable security controls and Army implementation procedures in the DoD RMF KS. Use the official DoD standard notice and consent language posted to the DoD RMF KS.

(11) Identification of ports, protocols, and services is required under DoD 8551.01 and NIST controls.

4-2. Protect Function

The protect function identifies the requirements to limit or reduce the impact of a potential cybersecurity event.

a. Control Access to IT and Information. Limit access to assets, systems, information, services, and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions. Required activities include--

(1) Actively manage the creation, deletion, use, dormancy and deletion of system and application accounts.

(2) Utilize standardized enterprise architecture and IT service management processes with technical enforcement, in order to secure and control access to IT assets, to include information, systems, and other resources.

(3) Allow only authorized access, employing the principles of least privilege and separation of duties, to users who are necessary to accomplish assigned tasks, in accordance with organizational missions and business functions.

(a) Least privilege. Grant users only the access they need to perform their official duties. (Mirroring users is discouraged and will not be utilized).

(b) Separation of duties. Divide roles and responsibilities so that a single individual cannot subvert a critical process. Document and divide mission functions amongst individuals by specifying the scenarios that require separation of duties and what would qualify as meeting the requirement. Update those functions to ensure the system is designed and configured to enforce separation of duties requirements.

(4) CISO is responsible for approving access permissions and monitoring users to ensure they continue to meet the requirements for their access type.

(5) Track, control, and enforce the use, assignment, and configuration of administrative privileges on computers, networks, and applications through automated, technical controls to the greatest extent possible in order to prevent unauthorized use.

(6) Address insider threats in accordance with policy and procedures in DODD 5205.16.

(7) Enforce identity management in order to ensure reliable authentication methods and enable accountability for all IT.

(8) Protect the integrity and availability of publicly available applications and information.

(9) Ensure appropriate access to information resources by foreign persons is only provided subject to

applicable DOD issuances.

(10) IT infrastructure changes must be authorized through the official change management process as defined in the approved authorization to operate, in accordance with DoDI 8510.01. Approved IT infrastructure changes will be implemented by authorized personnel and will be supervised by at least one additional authorized personnel to meet theTwo Person Integrity (TPI) requirements at all times.

(11) Protect classified IT systems and information from Insider Threats (InT) with the required comprehensive administrative, operational, and technical security measures.

b. Workforce management, training, education, and certification. Provide USAREC personnel and partners with Cybersecurity awareness education and training to perform their cybersecurity-related duties and responsibilities consistent with related DoD and USAREC issuances. Requirements include--

(1) Manage Cybersecurity workforce as defined in DoD 8140.01 the 8140.01 definition of cyberspace workforce will replace the current definition of IA workforce.

(2) USAREC civilian, military, and contracted support personnel assigned to perform cyberspace work roles will meet qualification standards established in DoD 8570.01-M, and supporting issuances, in addition to other existing workforce qualification and training requirements assigned to billets and position requirements.

(3) USAREC contracting officials will apply the Defense Federal Acquisition Regulation (DFAR) for contracted support designated to perform cyberspace workforce roles.

(4) All authorized users of IT systems will complete initial cybersecurity awareness training as a condition of access, and thereafter must complete annual cybersecurity awareness refresher training. All users must obtain the appropriate clearance and need-to-know for the system or network prior to gaining access.

(5) Privileged users obtain the appropriate certification for their work role in accordance with DoD 8570.01-M and its issuances.

(6) Organizations provide – in addition to DoD-mandated cybersecurity awareness training – USAREC-specific, mission-specific, system-specific orientation, training, awareness, and reinforcement programs to authorized users of IT as required to comply with this regulation.

(7) All USAREC personnel must document, monitor, update, and retain their training and certification status on ATCTS (https://atc.us.army.mil).

c. Data Security. Safeguard information and records (data) in accordance with applicable NIST, DoD and Army issuances. Required activities include--

(1) Assign all DoD and Army information in electronic format an appropriate level of confidentiality, integrity, and availability that reflects the importance of both information sharing and protection in accordance with DoDI 8510.01.

(2) Manage information and data to protect its confidentiality and integrity.

(3) Leverage processes and tools to prevent data exfiltration, mitigate the effects of data exfiltration, confidentiality and integrity of sensitive information.

(4) Leverage protective processes and tools to secure data at conception, in transit, at rest, and throughout the entire lifecycle.

(5) Protect transmission of information through appropriate COMSEC measures and procedures set forth in DoDI and applicable NIST, CNSS, DoD and Army issuances.

(a) For IT processing classified information, use only COMSEC, CHVP or Commercial Solutions for Classified (CSfC) products and services approved by National Security Agency/Central Security Service (NSA/CSS).

(b) For IT processing, sensitive information or information not approved for public release, use only COMSEC, CHVP or CSfC products and services approved by the NSA/CSS or those that National Information Assurance Partnership (NIAP). “This recognizes the protection of 'FOUO" is necessary, however the level of encryption does not have to meet that of the "classified.”

(c) If no listed COMSEC product meets the organization’s requirement, coordinate with the Army CIO to sponsor a product for testing that does meet the requirement. The sponsoring organization will reimburse the respective labs for costs associated with testing and evaluation.

(d) Submit requests through USAREC CIO to Army CIO for NSA services.

(e) Implement key and certificate management planning on COMSEC products and services in the Army infrastructure. This includes activities that involve the handling of cryptographic keys and other related security parameters (for example, IDs and passwords) during the entire lifecycle of the keys, to include their generation, distribution, storage, accounting, establishment, and destruction.

(6) Leverage integrity- checking mechanisms in order to verify the integrity of IT and data.

(7) Separate – physically or logically – development, test, user acceptance, and production environments in accordance with DISA guidance.

(8) Deny unauthorized persons information derived from telecommunications; and ensure the authenticity of classified or sensitive information – the loss of which would adversely affect the national security interest.

(9) Apply security measures to communications and IT that generate, handle, store, process, or use classified or sensitive information-the loss of which would adversely affect the national security interest.

(10) Ensure that IT components, associated data communications, and networks are protected in accordance with national emissions, TEMPEST AR 380-27 and procedures based on the security category or classification of the information.

d. Information Protection Processes and Procedures. Manage protection of IT and information. Required activities include--

(1) Properly and adequately safeguard Army and DoD-originated information residing on mission partner IT, with documented agreements indicating required levels of protection.

(2) Ensure that maintenance and disposal of information on IT complies with the provisions of DoDD 5015.2 and NIST SP 800-88.

(3) Integrate qualified cybersecurity personnel into all phases of the system development lifecycle.

(4) Track, control, and enforce the use, assignment, and configuration of administrative privileges on computers, networks, and applications through automated, technical controls to the greatest extent possible in order to prevent unauthorized use.

(5) Submit lessons learned for protective technologies to the Center for Army Lessons Learned.

(6) Regularly conduct, maintain, and test information backups.

(7) Ensure services that provide cross domain capabilities, including IT systems, automated data transfers, and manual data transfers, comply with provisions outlined in DODI 8540.01, DA PAM 25-2 Cross Domain Solutions and Data Transfer Management, and applicable DOD and joint issuances.

e. Maintenance of IT. Required activities include--

(1) Maintain and repair IT in a manner that prevents unauthorized access consistent with processes and procedures outlined within DoD and Army policies.

(2) Ensure COMSEC equipment users and maintenance technicians have been trained and certified to use and maintain COMSEC equipment in accordance with related CNSS, DoD and Army issuances.

(3) Identify, implement, control, and routinely monitor the use of Army-approved IT maintenance tools and remotely executed maintenance and diagnostic activities.

(4) Schedule, perform, and document system maintenance in a timely manner, in accordance with manufacturer or vendor specifications and/or organizational requirements. Maintenance includes software patching and meeting current NIST standards.

(5) Maintain current, accurate, and complete records of all maintenance and repair actions requested, scheduled, in-process and completed for the period of time defined by DoD policy and directives.

(6) Archive information, remove maintenance tools and destroy equipment containing organizational information, consistent with DoD and Army policies such as DOD Manual 5200.01, Volume 3, February 24, 2012, Incorporating Change 2, March 19, 2013 with particular attention to Enclosure 7, IT issues for the Security Manager. Other policy documents include Committee on National Security Systems Instruction 4004.1, Destruction and Emergency Protection for COMSEC and Classified Material, August 2006 With ANNEX B as amended 9 Jan 08; and AR 380-5, Department of the Army Information Security Program, with particular attention to 3-16 (Appropriate material destruction techniques and methods for non-paper-based material), subparagraph f (Equipment and f. Device Technology. Manage technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Required activities include

f. Use protective technologies and perform protective activities consistent with the Army’s and the organization’s risk strategy to ensure the security and resilience of systems and assets.

g. Collect and keep audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under his or her purview, and provide this data to appropriate LE or other investigating agencies.

h. Limit audit access to databases containing PII in order to ensure confidentiality while effectively implementing cybersecurity principles.

i. Implement technology components (for example, hardware and software) that have the ability to predict, prevent, reconfigure, optimize, self-defend, and recover with little or no human intervention. Attempts made to reconfigure, self-defend, and recover may produce an incident audit trail.

j. Use, mark, and protect authorized removable media in accordance with AR 380- 5 and relevant DoD and Army guidance.

k. Use the principle of least functionality, while enabling mission outcomes, in order to control access to systems and assets.

4-3. Detect Function

Detect is the ability to recognize a cybersecurity threat. Detection allows for the planning and documenting of a specific step-by-step process to mitigate and thwart a potential attack before it occurs. It also entails responding to alerts, compromised information, and anomalies. Active measures must be able to determine the extent, intensity, and impact of the attack. This function involves implementing a plan of action based on the assessments of vulnerabilities. This is important in network operations and is a critical component of Network Security and Vulnerability assessments. Detection ensures that Army networks operate free of intrusions and unauthorized software.

a. Anomalies and Events. Detect anomalous activity in a timely manner and understand the potential impact of events. Required activities include--

(1) Define and implement criteria and procedures to report problems identified, to include problem classification, categorization, mission impact, and prioritization.

(2) Identify problems through the correlation of incident reports, error logs, and other problem identification resources. Determine priority levels and categorization to address problems in a timely manner based on business risk and service definition.

(3) Prepare, maintain, and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.

(4) Establish, monitor, and manage a baseline of network operations and expected data flows for users and systems.

(5) Detect anomalies and changes in the organization’s environments of operation and IT, visibility into assets, awareness of vulnerabilities, knowledge of threats, security control effectiveness, and security status to include compliance.

(6) Analyze detected events in order to understand attack targets and methods.

(7) Employ authorized software that automates the process of monitoring the events occurring in a computer system or network, analyze them for signs of possible incidents, and attempt to stop possible incidents that are detected.

(8) Employ tools and technologies to monitor and detect events based on known attack signature as well as to detect anomalies in behavior or performance that could indicate an attack.

(9) Aggregate and correlate event data from multiple sources and sensors, and determine the impact of events.

(10) Increase situational awareness through enhanced monitoring capabilities and to subsequently increase insight into and control of the processes used to manage organizational security.

b. Continuous Monitoring. Monitor IT at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Required activities include--

(1) Establish a continuous monitoring strategy for IT that reflects the risk management strategy and organizational commitment to protecting critical missions and business functions.

(2) When IT permits, monitor continuously, in real-time, IT in order to determine the ongoing effectiveness of deployed security controls, changes in IT, and environments of operation, as well as compliance with legislation, directives, policies, and standards.

(3) Employ an effective continuous monitoring program that includes configuration management and control processes, security impact analyses, assessment of security controls employed, with metrics and security status reporting to appropriate organizational officials.

(4) Employ assessors or an assessment team to monitor, correlate, and analyze information generated by

assessments and monitoring to ensure that they are compliant.

(5) Discuss and share IT security status analysis results with appropriate parties.

(6) Employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

(7) Establish a continuous monitoring strategy for assessing a subset of the security controls employed within and inherited by the system during the authorization period.

(8) Employ incident management tools to assist in detecting, responding to, and limiting the consequences of a malicious cyber-attack against the organization.

(9) Regularly review and update the continuous monitoring strategy and program to increase visibility into assets and awareness of vulnerabilities.

(10) Monitor the infrastructure for unauthorized access, using approved intrusion detection tools, and ensure that any events are integrated with general event monitoring and incident management.

(11) Implement and maintain preventive, detective, and corrective measures (especially up-to date security patches and virus control) across the enterprise to protect IT and technology from malware (for example, viruses, worms, spyware, spam).

(12) Collect and process performance and conformance data.

(13) Implement policies and procedures that describe when, how, and what type of work can be performed or augmented by military, civilian, and contractor personnel, in accordance with the Army's enterprise-wide IT procurement policy and the IT control framework.

(14) Obtain formal agreement from contractors at the commencement of a contract, and existing contracts, that they are required to comply with the DoD RMF and relevant DoD and Army policies, such as policies for personnel security clearance, physical and logical access control, use of facilities, information confidentiality requirements, and non-disclosure agreements.

(15) Manage operations and establish network monitoring for users and systems.

(16) Ensure that cybersecurity personnel proactively conduct initial and periodic asset, vulnerability, and cybersecurity- based security assessments to detect IT vulnerabilities using approved tools, tactics, and techniques in order to facilitate the risk management process and to ensure compliance with network management.

(17) Monitor the infrastructure for unauthorized access and ensure that any events are integrated with general event monitoring and incident management.

(18) Monitor the physical environment to detect potential cybersecurity events.

(19) IT will be aligned to DoD network operations and security center (NOSC). The NOSC and supporting cybersecurity service provider(s) will provide any required cybersecurity services to aligned systems.

(20) DoDI 8530.01 applies to the DoDIN (including DoD owned IT, PIT systems, and Industrial Control Systems owned or operated by or on behalf of DoD components), cloud computing services (subject to the DoD Cloud Computing Services Requirements Guide), cleared defense contractors who operate pursuant to the DoD 5220.22 series and the National Industrial Security Program, and mission partner systems; but does not supersede existing DNI authorities over SCI systems. IT systems must be aligned to Defensive Cyber Operations Service Provider.

c. Detection Processes. Maintain and test detection processes and procedures to ensure timely and adequate awareness of anomalous events. Required activities include--

(1) Maintain a Cybersecurity plan that describes risk management processes, and how those processes align with the enterprise strategy and architecture. Build security improvement recommendations on approved business cases and implement the improvements as an integral part of services and solutions development, then operate using them as an integral part of business operations.

(2) Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against mission needs and operational requirements.

(3) Ensure measures are in place to detect and minimize unauthorized access, malicious, or non-malicious modification, or destruction of data.

(4) Ensure accountability via well-defined roles and responsibilities for detection.

(5) Conduct regular management reviews of the continuity capability in order to ensure its continued suitaability, adequacy, and effectiveness.

(6) Review the continuity plan on a regular basis to consider the impact of new or major changes to enterprise organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems, and application systems.

(7) Implement, maintain, and test detection processes and procedures to ensure timely and adequate awareness of anomalous cybersecurity events.

(8) Ensure detection activities comply with all applicable requirements.

(9) Communicate event detection information to appropriate parties in a timely manner in order to continuously improve detection processes.

(10) Coordinate for detection process metrics through the chain of command leadership so that standardized metrics are used throughout the Army. The frequency of testing Detection Processes will be will be promulgated as necessary with TRADOC and other stakeholders.

(11) Implement detection tools, technologies, and manual and/or automated methodologies within the context of an architecture designed to deliver the required information in the appropriate context and at the right frequencies.

(12) Manage records of events occurring within the organization’s systems and networks and ensure the integrity of the generation, transmission, storage, analysis, and disposal of security log data.

(13) Integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit records (logs) information through the use of a centralized logging software that can facilitate aggregation and consolidation of logs from multiple IT components.

4-4. Response Function

The activities in the respond function develop and implement the appropriate actions to contain, eliminate, and minimize the impact to Army systems, assets, data, and capabilities in order to safeguard mission essential functions, following a detected cybersecurity event.

a. Response Planning. Document, execute, and maintain response processes and procedures to ensure a timely response during or after a detected cybersecurity event. Protect the organization’s information and reputation by developing and implementing an incident response infrastructure (for example, plans, defined roles, training, communications, management oversight) for quickly discovering an attack and effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the Army network and systems. In conjunction with authorized and designated cybersecurity service providers.

(1) Establish a formal risk management approach, ensuring that it includes identifying, analyzing, responding to, mitigating, monitoring, and controlling risk.

(2) Assign properly trained personnel to execute the Army's risk management enterprise.

(3) All Army/Data owners must be identified in accordance with AR 25-1 and the Army Data Board. AOs will make risk management decisions, to include decisions to avoid, accept or mitigate risk, and then ensure those decisions are implemented.

(4) Maintain and review threat logs of known and identified attacks and their resolutions. Periodically analyze the logs for trends or recurring problems to identify and correct root causes, or to implement mitigation solutions.

(5) Business Continuity and Disaster Recovery Planning. All organizations (all Army/data owners) need to consider the response capability as part of the definition, design and development of mission business process and IT.

b. Communications. Coordinate response activities with internal and external stakeholders, as appropriate, to include external support from LE agencies. Required activities include--

(1) Ensure all personnel know their roles and responsibilities and order of operations when a response is required.

(2) Report incident events in a manner consistent with established reporting criteria.

(3) Share event information with all necessary personnel and organizations in accordance with response plans.

(4) Coordinate with stakeholders per the established response plan.

(5) Share information with external stakeholders in order to achieve broader cybersecurity situational awareness.

c. Analysis. Conduct analysis to ensure adequate response and support recovery activities. Required activities include-

(1) Calculate incident response and recovery impact (to include cost estimate, remediation, second and third order operational effects, as well as mission impact).

(2) Investigate notifications from automated detection systems.

(3) Conduct and understand impact analysis.

(4) Perform necessary forensics/investigation, root cause analysis, and TTPs to collect and gather

required incident information.

(5) Categorize incidents consistent with CJCSM 6510.01B, Cyber Incident Handling Program guidelines in order to help detect, deter, understand, and/or recover from attacks.

(6) Conduct vulnerability analysis of software throughout the lifecycle, using automated tools to the extent feasible. Software vulnerabilities that present unnecessary risk will be remediated to a level of acceptable risk as defined by DoD policy, DISA STIGs and USCYBERCOM operational orders.

d. Mitigation. Prevent expansion of an event, mitigate its effects, and eradicate the incident. Required activities include--

(1) Contain and handle incidents at the appropriate level.

(2) Take steps necessary to mitigate incident occurrences.

(3) Mitigate, document, and incorporate newly identified vulnerabilities into updated response planning.

(4) Utilize the guidelines described in NIST SP 800-61R2: Computer Security Incident Handling Guide.

(5) Have security authorization packages approved by the designated Authorizing Official that capture and identify the remaining vulnerabilities inherent to that baseline release and quantifies the residual risk. Any release of a baseline (system, OS, application, etc.) must be accompanied by a security authorization package approved by the designated Authorizing Official. The security authorization package must document residual risk to include all remaining vulnerabilities and the plan of action and POA&M for addressing these in accordance with DoDI 8510.01 and DoD RMF KS guidance.

e. Improvements. Improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into lessons learned. Update response strategies utilizing information from lessons learned.

4-5. Recover Function

The activities in the Recover function support the development, implementation, and maintenance of plans for operational resilience, continuity of operations (COOP), and the restoration of any capabilities or services that have been impaired due to a cybersecurity event.

a. Recovery Planning. Develop recovery plans that include the processes and procedures to be executed and maintained in order to ensure timely restoration of affected systems or assets, to reduce the impact from cybersecurity events. The goal of recovery planning is to ensure the ability of IT to operate under adverse conditions or stress, even if degraded or in a debilitated state, while maintaining essential operational capabilities and an acceptable level of risk, and to recover to an effective operational posture in a time frame consistent with mission needs.

(1) Maintain plans for resilience and restoration of any capabilities or services that are impaired due to a cybersecurity event. Ensure all IT Business Continuity Plans address cyber resilience requirements and are synchronized and tested with the Commands overall COOP Plan as an annex or appendix. The IT contingency plan will—

(a) Address maintaining essential missions and business functions despite an IT disruption, compromise, or failure, in accordance with the applicable NIST, DoD, and Army issuances. The plan will address eventual, full IT restoration without deterioration of the security safeguards originally planned and implemented, and must be reviewed and approved by the appropriate personnel and roles in accordance with DoDI 8510.01 and AR 500-3.

(b) Ensure system recovery processes are monitored and that security features and procedures are properly restored.

(c) Ensure IT recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, guidelines and ATOs.

(d) Provide for the execution and maintenance of recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events.

(e) Implement recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or alternate location.

(1) Execute recovery plans during or after an event.

(2) Capture written recovery plans in a straightforward, step-by-step style to minimize difficulty or confusion during an emergency.

(3) Implement interim measures to recover IT services following an emergency or IT disruption.

(4) Regularly test backup and recovery processes to ensure correct data storage, and to ensure information and system software may be restored without errors or lost data. IT recovery must be on an alternate operating environment from original system.

(5) Consider, where appropriate, a recovery plan for recovering one or more IT at an alternate facility in response to a major hardware or software failure or destruction of facilities.

(6) Write activities and procedures at a level at which an appropriately skilled technician can recover the system without intimate system knowledge.

(7) Restore operability of the target system, application, or computer facility infrastructure for mission/business processes or mission essential functions at an alternate location, per the recovery plan.

(8) Ensure appropriate personnel provide the procedures for relocating IT operations to an alternate location, where appropriate, and implement the procedures after major system disruptions.

(9) Ensure the roles and responsibilities of responders include one or more processes to verify the successful completion of the backup process, and address any backup failures.

(10) Test recovery plans at least annually.

(11) Implement a contingency plan for IT and distributes that plan to key recovery personnel. Cybersecurity personnel will--

(a) Coordinate recovery planning activities with incident handling activities.

(b) Review the recovery plan for the IT regularly.

(c) Update the contingency plan to address changes to the organization, IT, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

(12) Communicate contingency plan changes to the appropriate key contingency personnel.

(13) Protect the recovery plan from unauthorized disclosure and modification.

(14) Execute disaster recovery exercises periodically and implement corrective actions based on exercise results. Coordinate disaster recovery exercises with key recovery personnel. Refer to DA Pamphlet (PAM) 25-2, IT Contingency Planning for additional guidance on planning and conduction exercises.

(15) Ensure that a disaster recovery capability system is in place and tested sufficiently to ensure the ability to continue to fulfill mission-essential functions in the event of a disaster.

(16) Ensure IT recovery processes are monitored and cybersecurity features and procedures are properly restored.

(17) Provide for the smooth transfer of all mission-essential functions to an alternate site for the duration of an event with little or no loss of operational continuity when required.

(18) Include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance in disaster recovery procedures.

(19) Ensure that recovery is performed in a secure and verifiable manner. Document circumstances that can inhibit a trusted recovery, and put in place appropriate mitigating procedures.

(20) Store recovery media off-site at a location that affords protection of the data in accordance with its security categorization.

b. Improvements. Improve recovery plans and processes through the incorporation of lessons learned into future activities. Required activities include--

(1) Improve recovery planning and processes by incorporating lessons learned into future activities.

(2) Update recovery strategies regularly.

(3) Incorporate recommendations from the Cyber Center of Excellence and Center for Lessons Learned into recovery plans, and leverage information to prevent re-occurrences and improve processes.

(4) Ensure the authorizing official receives a Security Assessment Report (SAR) as required and is in accordance with DoDI 8510.01.

c. Centers, Cybersecurity Service Providers, and Internet Service Providers, and vendors. Communicate recovery activities to internal stakeholders and leadership in accordance with the recovery plan. Required activities include--

(1) Communicate recovery activities to internal stakeholders and executive and management teams.

(2) Develop, document, and disseminate procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and the organization must maintain current reviews and updates.

(3) Develop, document, and disseminate system and communications protection procedures that permit communications to vendors or contractors for official business, and implement encryption and control measures appropriate for the sensitivity of the information transmitted.

(4) Protect transmission of DoD information using COMSEC measures and procedures in accordance with DoDI and CNSS COMSEC policy documents as issued.

(a) Protect classified national security information using NSA-approved cryptographic and key management systems that offer high protection levels and are approved for protecting classified information.

(b) Protect CUI and PII using cryptographic and key management systems that comply with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11.

(c) Protect CUI and PII in transit and at rest in accordance with DoDI 8500.1 and DOD CIO Memorandum,

"Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media."

(d) Ensure services that provide cross domain capabilities, including IT systems, automated data transfers, and manual data transfers, comply with provisions outlined in DODI 8540.01, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02d, and DA PAM 25-2 Cross Domain Solution and Data Transfer Management.

d. Voice Communications. Voice communications must be protected consistent with the information transmitted. Required activities include

(1) Protect transmission of DoD classified voice communications with approved security services and/or equipment. NSTISSP No.101, "National Policy on Securing Voice Communications" outlines national policy on secure voice communications.

(2) Utilize Federal Information Processing Standard (FIPS) 140-2 to encrypt transmission of CUI voice communications.

(3) Protect all communications links of applicable U.S. government-owned or controlled space systems from exploitation, corruption, or denial consistent with mission requirements and the projected threat over the lifecycles of those space systems in accordance with Committee on National Security Systems Policy (CNSSP) No. 12,"National Information Assurance Policy for Space Systems Used to Support National Security Missions."

(4) Ensure the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Chapter 5.
User Agreements

Authorized users will sign a user agreement (paper or electronic) prior to account activation, annually thereafter, and whenever the baseline or applicable supplemental user agreement is revised.

a. Users will sign the agreement acknowledging that they--

(1) Have read, understood and agree to abide by their responsibilities and the rules of behavior with regard to IT usage and information handling in accordance with this regulation and associated DA PAMs.

(2) Have read, understood and agree to the notice of privacy rights and consent to authorize monitoring and searches in accordance with this regulation.

(3) Have read, understand and accept that violations of their responsibilities, unacceptable use of IT and/or mishandling of information may be punishable by administrative and/or judicial sanctions, may result in revocation or suspension of authorized access, may require remedial training in order to regain access, and/or may negatively influence adjudication decisions of security clearances.

b. The USAREC CISO utilizing the Army CIOs will publish the baseline user agreement and annually revise and update the baseline user agreement as required. The baseline user agreement will provide the minimum requirements that govern the appropriate use of IT and will be included in all IT user agreements.

c. Organizations can develop supplemental rules to address mission and function specific requirements. A. copy of the supplemental rules will be provided to the Army CIO.

d. Organizations will track the issuance, signing, and periodic reviews of user agreements for all users under their management control. A copy of the signed acknowledgement will be added to the user's ATCTS profile.

5-1. User Responsibilities and Rules of Behavior

All personnel, to include authorized and privileged users, will comply with their responsibilities and this regulation. These responsibilities and rules of behavior are in place to help protect the confidentiality, integrity, and availability of IT and information. Noncompliance with laws, DoD and Army regulations pertaining to the use of IT and handling of information may raise security concerns about an individual's reliability and trustworthiness for access to IT and information.

a. Access to DoD and Army IT and information is for official use and authorized purposes only, as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy. Official use is defined as use necessary to further an Army interest or otherwise directly related to the conduct of the Army business, or having an indirect impact on the ability to conduct Army business, and includes emergency communications and communications necessary to carry out the business of the Federal government. Authorized use must not adversely affect the performance of official duties or degrade IT performance, must be of reasonable duration and frequency as determined by commanding officers and supervisors, and does not violate user responsibilities or the rules of behavior.

b. Military, civilian, and contractor personnel may be subject to administrative and/or judicial sanctions if they knowingly, willingly or negligently compromise, damage, or place IT or information at risk by violating the user agreement. Individuals involved with misuse of the IT or violation of prohibited activities may be subject to having computer account access suspended for a defined period of time and/or required to complete the appropriate remedial training.

5-2. Notice of Privacy Rights and Authorized Monitoring and Searches.

Consistent with the DoD Banner and User Agreement, any use of Army IT is made with the understanding that users will have no expectations as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses. The Army reserves and will exercise the right to access, intercept, inspect, record, and disclose any and all electronic communications on Army IT, including minor incidental personal uses, at any time, with or without notice to anyone, unless prohibited by law or privilege.

Chapter 6.
Acquisition/Procurement of IT Solutions

a. Program Managers (PMs), or Information System Owners (ISOs) when there is no identified PM, must develop, implement, and maintain an effective cybersecurity strategy that is consistent with DoD policies, procedures, standards, and other guidance.

b. PMs, or ISOs when there is no identified PM, will integrate DoDI 8510.01 activities with acquisition processes for all IT-enabled systems, to ensure that overall risk of the system is determined to be acceptable according to DoD risk acceptance guidance, Joint Capabilities Integration Development System (JCIDS) key performance parameters and NIST standards.

c. PMs, or ISOs when there is no identified PM, must develop, implement, and maintain countermeasures that address the risks to their systems, products, and applications so as to achieve mission assurance with the lowest level of risk feasible. Countermeasures will address anti-tamper, cybersecurity, operations security, information security, personnel security, and physical security, secure system design, supply chain risk management, software assurance, anti- counterfeit practices, procurement strategies, and other mitigations in accordance with DoDI 5200.39, DoDI 5200.44, and DoDI 8500.01, as appropriate, so as to achieve an acceptable level of risk, as described in DoDI 8510.01, such that the need to accept high risk is eliminated.

d. All IT must be acquired in accordance with public law and have been evaluated and validated in accordance with appropriate NIST, DoD and Army issuances before purchase.

e. IT capabilities that are acquired or provided as a service must align to the DoD's Information Enterprise and the Joint Information Environment in accordance with DoDI 5000.74, Defense Acquisition of Services.

6-1. IT Products

a. Network Technologies. The DOD Unified Capabilities (UC) Approved Products List (APL) is the authoritative list of products that have completed interoperability and cybersecurity certification and is available at https:// aplits.disa.mil.

(1) For IT products that support unified capabilities on the Army-managed portion of the DoDIN, excluding cryptologic SCI IT and classified cryptologic products, only those listed on the DoD UC APL are approved for purchase.

(2) IT products approved for purchase, i.e., those listed on the DoD UC APL must be procured through the Project Director, Computer Hardware and Enterprise Software Solutions (CHESS) contract vehicles. See PD CHESS website for further information (https://chess.army.mil).

(3) Requests for exemptions to purchase approved IT products not on the DoD UC APL will be made in accordance with DoDI 8100.04, Unified Capabilities.

(4) Only the Army CIO is authorized to approve requests for exemptions to the requirement to purchase IT products through PD CHESS.

b. COMSEC. In addition to NIST and DoD issuances, national security systems must comply with CNSS issuances related to COMSEC.

(1) For IT processing classified information, acquire/procure only COMSEC products and services approved by NSA/ CSS.

(2) For IT processing, sensitive information or information not approved for public release, acquire/procure only COMSEC products and services approved by the NSA/CSS or those that NIAP has issued a validation certificate for meeting the requirements for EAL 3 and the Common Criteria controlled access protection profile.

c. If no listed product meets the organization's requirement, coordinate with the Army CIO to sponsor a product for testing that does meet the requirement. The sponsoring organization will reimburse the respective labs for costs associated with testing and evaluation.

d. All products, once procured, will be marked with a USAREC Label 25-2.1 "Sensitive/Unclassified" label or a UF 25-2.2 " Sensitive/Unclassified (Authorized to travel) label.

6-2. IT Services

a. Leverage existing services. To the maximum extent practical, the PM, or ISO when there is no identified PM, should leverage existing IT services that may be shared within and among DoD components and among federal government agencies.

b. Use only authorized cloud service providers. Use of commercial cloud-based solutions and services that reduce cost of IT ownership is encouraged. However, only commercial Cloud Service Providers (CSP) who obtain and maintain a DoD Provisional Authority (PA) for their cloud service offerings are authorized for use.

6-3. Software

a. The Army will implement an enterprise-level approach to achieve alignment and integration of security requirements for inspection and oversight of component and Command traditional (information, personnel, physical and industrial) and Cybersecurity programs in order to identify compliance trends that present unacceptable Cybersecurity risk or result in inefficient use of resources by--

(1) Collecting data through automated processes whenever possible to limit disruption to the activities of the organization from whom the information is required and in support of continuous monitoring objectives.

(2) Conducting vulnerability assessments, intrusion assessments, penetration testing, other applicable activities (using internal or external capabilities) to provide a systemic view of IT current risk posture.

(3) leveraging data collected by existing DoD, Joint, and Army inspections, audits, investigations and program assessments whenever practical to inform compliance and risk assessments.

(4) Army activities will share applicable assessment results with the AENC, which will coordinate with Army stakeholders who have the authority to take appropriate action to resolve systemic issues and mitigate unacceptable risk. The purpose for sharing these results is not to support punitive or other negative action, but to identify and resolve systemic issues and mitigate unacceptable risk to missions and business functions. When requested, anonymity of the reporting organization will be preserved as much as possible in order to encourage reporting.

a. All IT will be assessed for interoperability and cybersecurity compliance and sustainment as part of the acquisition process. Interoperability and cybersecurity sustainment includes continued alignment with current industry best practices, including the ability to operate with vendor-supported applications and operating systems.

Chapter 7.
Reporting Requirements

Army Commands will report on the status of cybersecurity metrics when directed to ensure that leadership has useful, up-to-date information on the level of performance and existing gaps in their cybersecurity posture.

7-1. Statutory Requirements for Reporting Information Required by the Federal Information Security Modernization Act of 2014 (FISMA)

FISMA requires all federal agencies, departments, and their contractors to adequately safeguard their IT and assets. DoD must meet or exceed the standards required by the OMB and the Secretary of Commerce, pursuant to FISMA and section 11331 of Title 40, U.S.C. Commanders and senior leaders of agencies and activities who have the responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of IT will ensure IT under their purview complies with DoD 8510.01.

7-2. Privacy Impact Assessments

a. A privacy impact assessment will be conducted for data collection instruments that collect, maintain, use, and or disseminate personally identifiable information (PII) in an electronic form about members of the public, DoD personnel (government civilians, members of the military, and non-appropriated fund employees), contractors or foreign nationals employed at U.S. military facilities to assess whether the PII is collected, stored, or disseminated in a manner that protects the privacy of individuals and their information.

b. Privacy impact assessments will be completed in accordance with DoDI 5400.16, AR 25-1 and DA PAM 25-1-1 and documented on DD Form 2930.

7-3. Cybersecurity Readiness

Commanders will emphasize the importance of cybersecurity discipline within their organizations, and ensure their organizational inspection program assesses cybersecurity readiness and compliance with higher level risk management policy and guidance. Cybersecurity readiness assessments will be included in unit status reports.

7-4. Systemic or Critical Cybersecurity Issues

Systemic or critical Cybersecurity-related will be reported through via memorandum for the Army Office of the Chief Information Officer/G6 (SAIS-ZA), 107 Pentagon, Washington, DC 203-0107.

7-5. Cyber Events

Report suspected or confirmed incidents in accordance with Army regulations relevant to the specific incident, ARCYBER published procedures, and applicable Contingency of Operations (COOP) plans IAW AR 500-3, IT contingency plans IAW DA PAM 25-1-2, incident response plans and organizational policies and procedures.

Appendix A

References

Section I
Required Publications

See the DoD Cybersecurity Policy Chart at http://iac.dtic.mil for the DoD list of applicable cybersecurity policies, to include OSD, NIST, CNSS and other governing organizations.

AR 25-1
Army Information Technology (Cited in paras 2-10k, 2-10l, 2-10m, 4-4a.(3), 7-2b.)

AR 25-30
Army Publishing Program (Cited in para 3-1d.)

AR 380-5
Department of the Army Information Security Program (Cited in paras 4-2e. (6), and 4-2 e. (6) (e))

AR 380-67
Personnel Security Program (Cited in 2-11i)

AR 500-3
U.S. Army Continuity of Operations Program Policy and Planning (Cited in 4-5a. (1)(a), and 7-5)

DA PAM 25-1-1
Army Information Technology Implementation Instructions (Cited in para 3-1d)

USAREC Regulation 25-1
US Army Recruiting Command Information Technology (Cited in paragraphs 2-10o., and 2-10q.)

USAREC Pamphlet 25-1-1
USAREC Information Technology Implementation Instructions

Section II
Related Publications

AR 220-1
Army Unit Status Reporting and Force Registration Consolidated Policies

AR 380-40
Safeguarding and Controlling Communications Security Material

AR 735-5
Property Accountability Policies

DA PAM 25-2-1
Information Technology Contingency Planning

DA PAM 25-40
Army Publishing Program Procedures

DODD 5205.15
The DOD Insider Threat Program

DODD 8115.01
Information Technology Portfolio Management

DODD 8140.01
Cyberspace Workforce Management

DODI 8500.01
Cybersecurity

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT)

DODI 8520.02
Public Key Infrastructure (PKI) and Public Key (PK) Enabling

DODI 8520.03
Identity Authentication for Information Systems

DODI 8523.01
Communications Security (COMSEC)

DODI 8530.01
Cybersecurity Activities Support to DOD Information Network Operations

DODI 8540.01
Cross Domain (CD) Policy

DoDI 8551.01
Ports, Protocols, and Services Management.

USC 2222
Defense business systems: business process reengineering; enterprise architecture; management

U.S. Code 2551
Congressional statement of purpose

USC 791
Employment of Individuals with Disabilities

USC 794
Nondiscrimination under Federal grants and programs

USC 794d
Electronic and Information Technology

USC Subtitle III, Chapter 113
Responsibilities for Acquisitions of Information Technology

USC Chapter 35
Coordination of Federal Information Policy

USC 3544
Federal agency responsibilities

USC 3545
Annual independent evaluation

Section III

Prescribed Forms

USAREC Label 25-2.1
Sensitive/Unclassified Label (Prescribed in Chapter 6-1 d.)

USAREC Label 25-2.2
Sensitive/Unclassified Label (Authorized for travel) (Prescribed in Chapter 6-1 d.)

Section IV

Referenced Forms

DA Form 11-2
Internal Control Evaluation Certification (Available at http://www.apd.army.mil/pub/eforms/pdf/A11_2.pdf)

DA Form 2028
Recommended Changes to Publications and Blank Forms (Available at http://www.apd.army.mil/pub/eforms/pdf/ A2028.pdf)

DD Form 2875
System Authorization Access Request (SAAR)

DD Form 2930
Privacy Impact Assessment

Appendix B
Internal Control Evaluation

B–1. Function
The function covered by this checklist is the administration of Army cybersecurity in IM and IT organizations.

B–2. Purpose
The purpose of this checklist is to assist HQDA, ACOMs, ASCCs, DRUs, PEOs, PMs, and installations in evaluating the key internal controls listed. It is intended as a guide and does not cover all controls.

B–3. Instructions
Answers must be based on the actual testing of internal controls (such as document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation.

B–4. Test questions
a. Responsibilities. (Chapter 2)

(1) Are the duties and responsibilities of the senior information management official clearly designated in the organization's mission and function?

(2) Has the installation clearly established a NEC who has the sole responsibility of implementing the installation's cybersecurity program?

(3) Does the organization have a strategic plan that is linked to its missing? Is it periodically updated? (ACOM, ASCC, and DRU.)

(4) Is a Security Control Assessor appointed in writing?

b. Critical Infrastructure Framework (Chapter 4-8)

(1) Has a forum been established to develop and implement cybersecurity procedures, requirements, and priorities?

(2) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration?

(3) Does the IT investment screening process include addressing the questions in this checklist, resolving all issues prior to making an IT investment, and initiating any process analysis or improvement? (HQDA, ACOM, ASCC, and DRU.)

(4) Have appropriate security personnel (for example, ISSMs) been appointed?

(5) Have risk analyses been performed for systems that process, access, transmit, or store Army information?

(6) Are the appropriate leadership and management personnel aware of the results of risk analysis and risk assessments.

(7) Have security assessments been performed as per standard Army methodologies as detailed in this regulation to ensure consistency?

(8) Does the organization understand the cyber risk to organizational operations?

(9) Are access to assets and associated facilities limited to authorized users?

(10) Are the organization’s personnel and partners been provided cybersecurity awareness training? Personnel and partners been provided cybersecurity awareness training?

(11) Does the organization ensure its technical security solutions are consistent with policy and procedures?

(12) Is anomalous activity detected in a timely manner and its potential impact on systems clearly understood?

(13) Are response processes in place and adequately maintained to ensure timely response to detected cybersecurity events?

(14) Is there a plan in place to ensure response activities will be coordinated with internal and external stakeholders, to include external support from law enforcement?

(15) Are recovery planning and processes continuously evaluated for relevance and improvement?

B–5. Supersession

No supersession

Appendix C
Cyber Workgroup

C-1. Workgroup Statement:

a. The DCG-S is the Command Cyber Chair, the command is committed to preserving the confidentiality, integrity and availability of all forms of information used by the organization and maintained on behalf of employees, customers and government agencies. As a result, specific procedures are developed to help administer and manage the storage and processing of computer information and any non-computer information related to the proper and lawful conduct of mission related business. These procedures address all computer and information management activities that could constitute a threat or risk to the ongoing proper activities of this organization in such a way that risk is minimized or otherwise accepted by the executive officers of US Army Recruiting Command (USAREC).

b. The leader of the information security function is designated as the Chief Information Security Officer (CISO) under direction of the Chief Information Officer (CIO), the controlling officer in charge of developing, maintaining, disseminating and measuring compliance with this policy through the procedures and standards that are generated in response to this commitment.

c. To ensure that the importance of this workgroup is communicated uniformly throughout the organization, all Executive Leaders, CIO and CISO will at least annually, discuss and ratify this Workgroup as it relates to regulatory compliance, legal privacy protection and information protection.

d. This workgroup is applicable to all computer equipment, network or data communications equipment, computer programs, procedures and support software, data storage devices and media. Employees, business partners and contract personnel who use any computer-related technology must be aware of the provisions and their requirements related to this policy.

e. In addition, this workgroup authorizes the development of standards for personnel activities, incident prevention and reporting and compliance or audit reviews directed by appropriate regulations and commonly accepted business practices.

6. Changes necessary to reflect current technology and new methods for ensuring secure business procedures will be supplemented to existing procedures as often as necessary.

C-2. USAREC Cyber Work group:

a. Business Need for Security: USAREC owns significant assets in the form of information. Some of these assets lose significant value if they are improperly disclosed. Similar disclosure of other assets could result in significant harm to the command. Furthermore, unauthorized changes to the information content of these assets can damage the command's ability to perform business. Conversely, preventing authorized access to these assets can do significant harm. Leadership must ensure that information and information systems are properly protected from a variety of threats, including error, fraud, embezzlement, improper disclosure, sabotage, terrorism, extortion, espionage, privacy violation, service interruption and natural disaster.

b. Scope: All military personnel, civilian employees, contractors, part-time and temporary workers, and those employed by others to perform work on command’s premises or granted access to USAREC information or systems are covered by this policy. Any personnel not covered by this policy (for example, visitors) must be supervised by an employee at all times while they are on the command’s premises. Information regarding this policy and its implementation must be made available to down to the ever leader responsible for the performance of that unit member.

c. Roles and Duties of the Staff Responsible for Various Security Functions:

(1) All military personnel, civilian employees, contractors, and temporary and part-time workers are responsible for ensuring that command’s information assets are used only in proper pursuit of the command’s business; information is not improperly disclosed, modified or endangered; and access to command’s information resources is not made available to any unauthorized person.

(2) The Chief Information Security Officer (CISO) and team are responsible for ensuring that appropriate security controls are in existence and in force throughout the command. A security administration leadership function is responsible for ensuring that all authentication and authorization management systems are current and accurate. The security management function is responsible for determining methods of implementing and enforcing security policies and for advising resource owners on forming appropriate security policies. Application design and development staff members are responsible for ensuring that security policies are effectively and efficiently implemented within their applications and that those policies are administered.

(3) Any employee involved in selecting or purchasing computer systems or application software is responsible for ensuring that this policy can be effectively implemented for that system or application within the enterprise portfolio.

(4) CISO must evaluate all stored information, applications and information systems to determine the appropriate controls required to protect the information asset on the basis of its criticality to the business, value to USAREC, and potential value to adversaries. These evaluations will be documented and reviewed at least once annually. In addition, the CISO function will conduct ongoing reviews of risks to company information and systems.

(5) Each organization unit commander, director or leader will assign one or more managers the responsibility for resource ownership of those information assets housed or managed within their area of operation, as determined by the security management function.

d. Violation Reporting and Escalation: Any person covered by this regulation is obligated to report apparent violations of this policy to the responsible commander, director or leader. If the violation does not appear to be resolved in a timely manner, the CISO team leadership must be notified by the person observing the violation. Report violations via email to USARMY Ft Knox USAREC Mailbox HQ G6 IA Office.

e. Legal or Regulatory Requirements: USAREC continuously endeavors to comply with the information security requirements and implications of any applicable laws and regulations.

C-3. USAREC: Enterprise Information Security Charter Strategy

- Purpose — This workgroup presents the philosophy of information security within the United States Army Recruiting Command (USAREC) and represents the endorsement of the USAREC Leadership team. It identifies the motivation for security, describes information security principles and terms, and defines the scope of information security policies and responsibilities of the various security functions.
- Users — All military personnel, civilian employees, contractors and service providers of USAREC.
- Workgroup Owner — Chief Information Security Officer (CISO), under direction of the Chief Information Officer (CIO).

C-4. Workgroup Description

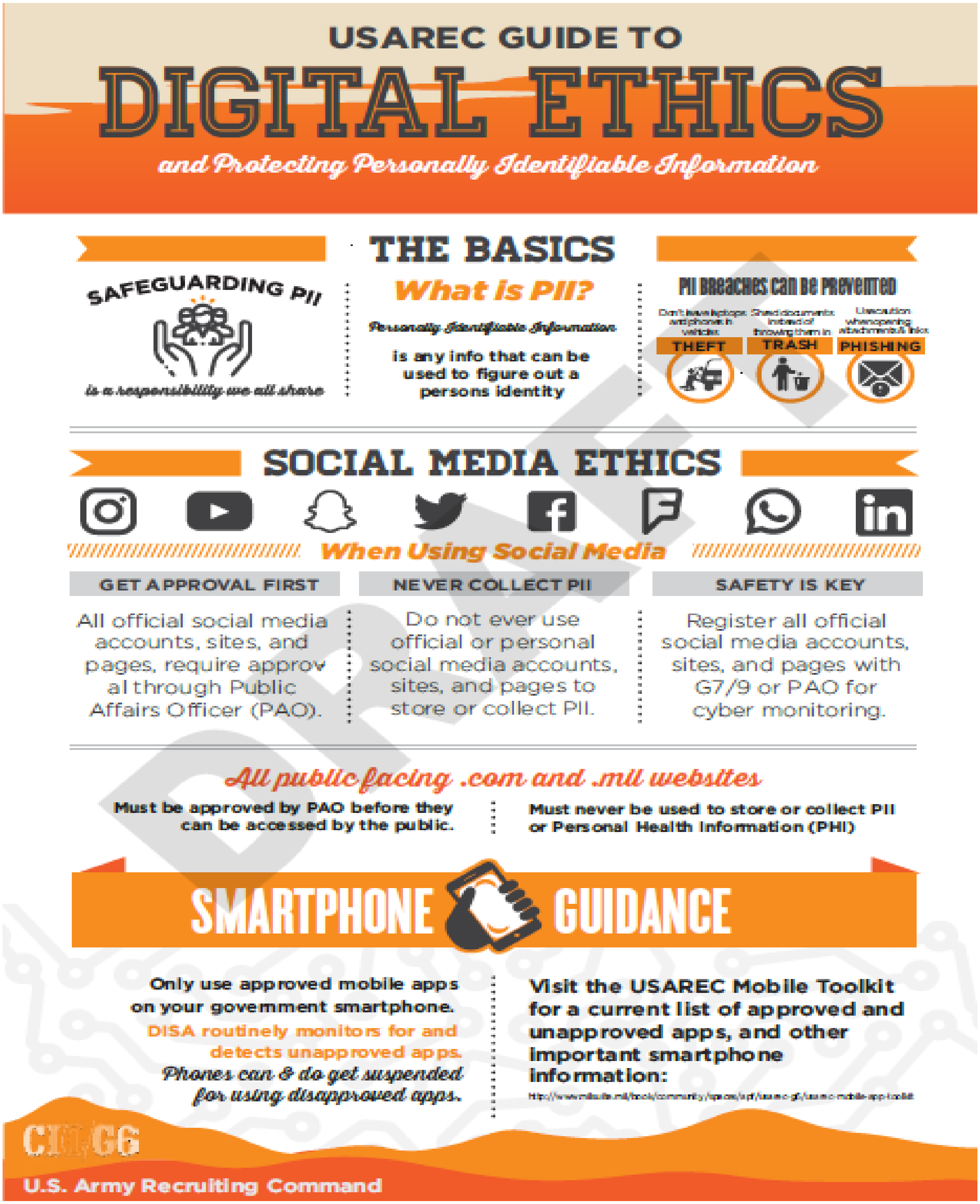
- Objective — USAREC recognizes that information and IT assets are critical business assets. It is the responsibility of all users to ensure the safeguarding of business assets. USAREC implements, maintains and monitors a comprehensive enterprise information security policy and compliance program appropriate to:
- The risks of the business
- Generally accepted information security practices
- Applicable legal and regulatory requirements
- **Motivation** — USAREC values the ability to openly communicate and share information. USAREC information (whether belonging to USAREC or held in trust on behalf of its clients and organizational partners) is an important asset that shall be protected according to its value and the degree of damage that could result from its misuse, unavailability, destruction, unauthorized disclosure or modification. Improper disclosure or destruction of these assets may result in harm to the U.S. Army and this command. Information assets are identified, valued, assessed for risk and protected as appropriate to the needs and risks of the business. Users are required to abide by this USAREC Information Security Charter and subsequent policies and procedures.
- **Principle Goals** — Information security is a risk management discipline addressing the preservation of information confidentiality, integrity and availability. The information security effort is established via a hierarchical set of policies and procedures that help users and administrators to define and mitigate risks, maintaining a trade-off between information value and cost of risk mitigation. Policies are high-level documents used to put information security principles into practice. Procedures are a series of related activities aimed at achieving a set of objectives in a measurable and repeatable manner.
- **Principle 1** — Information security policies, standards, guidelines and procedures are developed to communicate security requirements and guide the selection and implementation of security control measures.
- **Principle 2** — Personal accountability and responsibility for information security are incorporated in roles and responsibilities that ensure that every individual applies the applicable information security policies, principles, procedures and practices in their daily work-related activities.
- **Principle 3** — Information security education, training and awareness programs ensure that users are aware of security threats and concerns and are equipped to apply organizational security policies and principles.
- **Principle 4** — Information assets are classified according to their criticality to the organization enabling an appropriate level of protection.
- **Principle 5** — Information assets are to be used for intended business purposes only.
- **Principle 6** — Legal, regulatory and contractual requirements are identified, documented and followed.
- **Principle 7** — Response, USAREC must meet required reporting requirements and timelines. Must be agile to respond in real time.
- **Principle 8** — Maintain, USARECs Eight (8) Target, Priority and Domain Technology areas. Public (.COM), Accountability, Certification and Training, Cyber Policy and Operations, Cyber Risk, Inspections and Audits, Theft and Loss (Physical Security) and Digital Risk Monitoring (Social Media).
- Maintain USARECs Cyber Score Card to be utilized as a tool to identify information security strengths, weakness and training opportunities.

- **Scope** — Information must be protected in whatever form, including, but not limited to, paper documents, electronic data and the spoken word. Information should be protected while at rest and when channeled, transmitted or conveyed. IT assets include all devices and hardware/software components of the IT infrastructure, applications and data stores.
- **Action** — All military personnel, civilian employees and contractors have a responsibility to report suspected security failures or policy violations.

C-5. Roles/Responsibilities

- **Executive Leaders** — Executive leaders are accountable for information security and must ensure compliance with security policies, standards, procedures and practices within their respective areas of responsibility.
- **Information Security Leadership** — The Chief Information Security Officer (CISO), under direction of the Chief Information Officer (CIO) is responsible for ensuring that appropriate security controls exist and are in force throughout the enterprise. The leader is responsible for determining methods of implementation and enforcement of security policies, and for advising the enterprise on security-related issues. The leader ensures, in particular, that information security awareness is increased, and audits are performed and reported regularly. The leader appoints and manages suitably skilled people to staff information security teams as deemed appropriate, and the leader has the authority to request the appointment of security representatives within the command.
- **Workgroup Security Policy and Compliance Governance** — Security policy and compliance governance is provided by a multidisciplinary group that reviews and endorses information security policy objectives and strategies. They agree to the roles and responsibilities for information security across the enterprise as defined in specific policies. They visibly promote and provide business support for information security initiatives throughout the enterprise. The governance group is led by the information security leader and includes representatives from all major business units.
- **Enforcement** — Any violation of this policy will be subject to disciplinary action, up to and including termination of employment.

Appendix D.
USAREC Guide to Digital Ethics and protecting Personally Identifiable Information (PII)



USAREC GUIDE TO DIGITAL ETHICS

and Protecting Personally Identifiable Information

THE BASICS

SAFEGUARDING PII

is a responsibility we all share

What is PII?

Personally Identifiable Information

is any info that can be used to figure out a persons identity

PII BREACHES CAN BE PREVENTED

Don't leave laptops and phones in vehicles	Shred documents instead of throwing them in	Use caution when opening attachments & links
THEFT	TRASH	PHISHING

SOCIAL MEDIA ETHICS

When Using Social Media

GET APPROVAL FIRST	NEVER COLLECT PII	SAFETY IS KEY
All official social media accounts, sites, and pages, require approv al through Public Affairs Officer (PAO).	Do not ever use official or personal social media accounts, sites, and pages to store or collect PII.	Register all official social media accounts, sites, and pages with G7/9 or PAO for cyber monitoring.

All public facing .com and .mil websites

Must be approved by PAO before they can be accessed by the public.

Must never be used to store or collect PII or Personal Health Information (PHI)

SMARTPHONE GUIDANCE

Only use approved mobile apps on your government smartphone.

DISA routinely monitors for and detects unapproved apps.

Phones can & do get suspended for using disapproved apps.

Visit the USAREC Mobile Toolkit for a current list of approved and unapproved apps, and other important smartphone information:

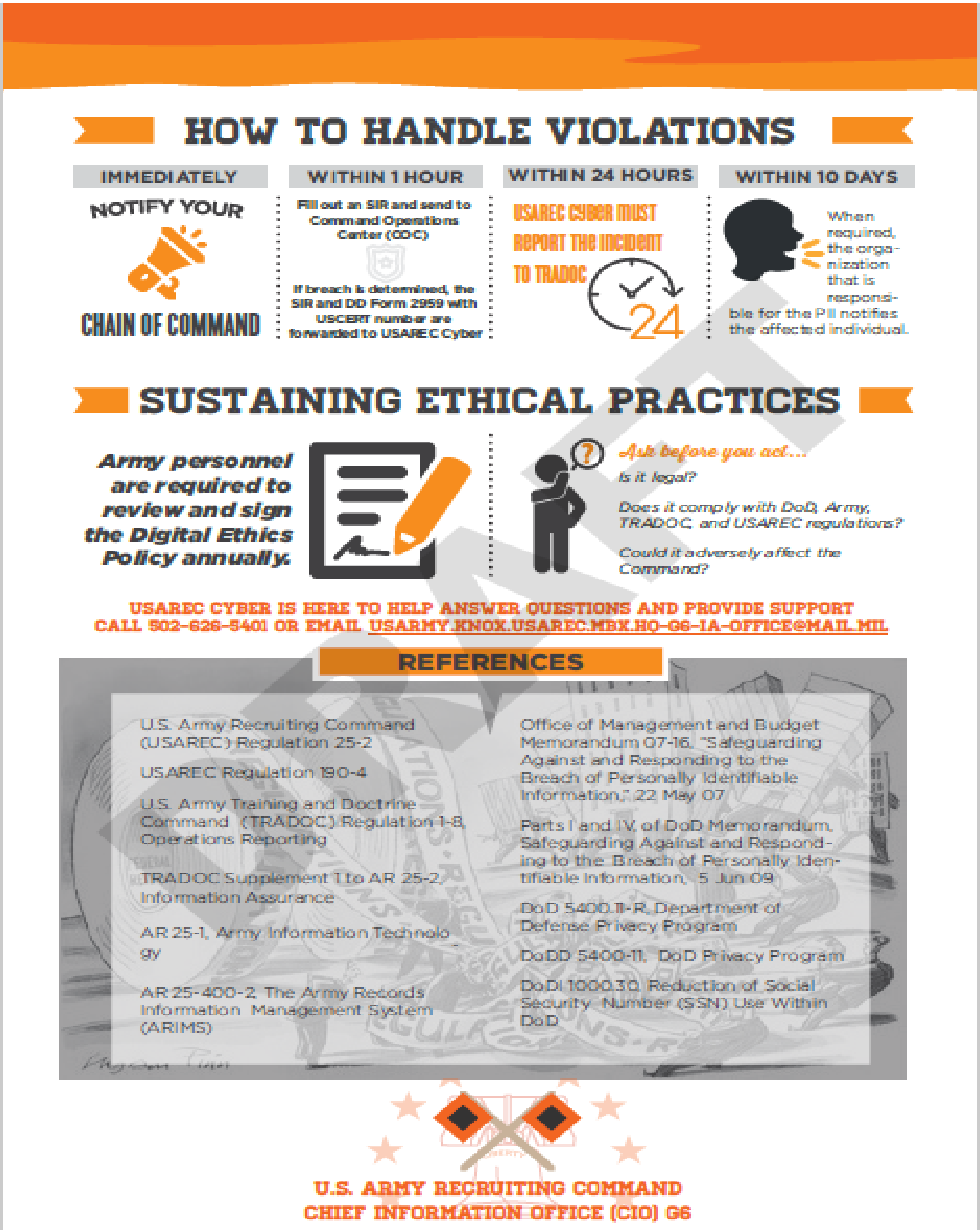
http://www.milsuite.mil/book/community/spaces/apf/usarec-g6/usarec-mobile-app-toolkit

CIO G6

U.S. Army Recruiting Command

(USAREC Guide to Digital Ethics, page 1)

USAREC Guide to Digital Ethics page 2.



HOW TO HANDLE VIOLATIONS

IMMEDIATELY

NOTIFY YOUR CHAIN OF COMMAND

WITHIN 1 HOUR

Fill out an SIR and send to Command Operations Center (COC)

If breach is determined, the SIR and DD Form 2959 with USCERT number are forwarded to USAREC Cyber

WITHIN 24 HOURS

USAREC CYBER MUST REPORT THE INCIDENT TO TRADOC

WITHIN 10 DAYS

When required, the organization that is responsible for the PII notifies the affected individual.

SUSTAINING ETHICAL PRACTICES

Army personnel are required to review and sign the Digital Ethics Policy annually.

Ask before you act...

Is it legal?

Does it comply with DoD, Army, TRADOC, and USAREC regulations?

Could it adversely affect the Command?

USAREC CYBER IS HERE TO HELP ANSWER QUESTIONS AND PROVIDE SUPPORT
CALL 502-626-5401 OR EMAIL USARMY.KNOX.USAREC.MBX.HQ-G6-IA-OFFICE@MAIL.MIL

REFERENCES

U.S. Army Recruiting Command (USAREC) Regulation 25-2

USAREC Regulation 190-4

U.S. Army Training and Doctrine Command (TRADOC) Regulation 1-8, Operations Reporting

TRADOC Supplement 1 to AR 25-2, Information Assurance

AR 25-1, Army Information Technology

AR 25-400-2, The Army Records Information Management System (ARIMS)

Office of Management and Budget Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," 22 May 07

Parts I and IV, of DoD Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 5 Jun 09

DoD 5400.11-R, Department of Defense Privacy Program

DoDD 5400-11, DoD Privacy Program

DoDI 1000.30, Reduction of Social Security Number (SSN) Use Within DoD

U.S. ARMY RECRUITING COMMAND
CHIEF INFORMATION OFFICE (CIO) G6

(USAREC Guide to Digital Ethics, page 2)

Glossary

Section I
Abbreviations

A&A
Assessment and Authorization

ACOM
Army Command

AENC
Army Enterprise Network Council

AIC
Army Interoperability Certification

AO
Authorizing Official

AR
Army Regulation

ARCYBER
Army Cyber Command

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics & Technology)

ASA (FM&C)
Assistant Secretary of the Army (Financial Management & Comptroller)

ASCC
Army Service Component Command

ATCTS
Army Training and Certification Tracking System. https://atc.us.army.mil

ATEC
Army Test and Evaluation Command

ATO
Authority to Operate

AUP
Acceptable Use Policy

BMA
Business Mission Area

CCI
Controlled Cryptographic Item

CD
Cross Domain

CDS
Cross Domain Solution

CG
Commanding General

CHVP
Cryptographic High Value Product

CID
Criminal Investigation Command

CIO
Chief Information Officer

CIO-EB
Chief Information Officer-Executive Board

CISO
Chief Information Security Officer

CJCSI
Chairman of the Joint Chiefs of Staff Instruction

CNSS
Committee on National Security Systems

CNSSD
Committee on National Security Systems Directive

CNSSI
Committee on National Security Systems Instruction

CNSSP
Committee on National Security Systems Policy

COMSEC
Communications Security

COOP
Continuity of Operations

CSfC
Commercial Solutions for Classified

CSID
Code Signing Identification

CUI
Controlled Unclassified Information

DCI
Data Collection Instrument

DCS, G–1
Deputy Chief of Staff, G–1

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3/5/7
Deputy Chief of Staff, G–3/5/7

DCS, G–4
Deputy Chief of Staff, G–4

DISA
Defense Information Systems Agency

DITPR
DoD IT Portfolio Repository

DoD
Department of Defense

DoDD
Department of Defense Directive

DoDI
Department of Defense Instruction

DoDM
Department of Defense Manual

DOT&E
Director, Operational Test & Evaluation

EIEMA
Enterprise Information Environment Mission Area

ESSG
Enterprise-wide IA and Computer Network Defense
Solutions Steering Group

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act of 2014

FO
Foreign Officials

HQDA
Headquarters, Department of the Army

IC
Intelligence Community

ICS
Industrial Control Systems

ILS
Integrated Logistics Support

INSCOM
Information Security Command

InT
Insider Threat

IRM
Information Resources Management

IS
Information System

ISO
Information System Owner

ISSO
Information System Security Officer

ISSPA
Army Information System Security Program Application

IT
Information Technology

LE
Law Enforcement

NDA
Non-disclosure Agreement

NEC
Network Enterprise Centers

IPRNet
Non-secure Internet Protocol Routing Network

NIST
National Institute of Standards & Technology

NSA
National Security Agency

NSA/CSS
National Security Agency/Central Security Services

NSS
National Security System

OMB
Office of Management and Budget

OPSEC
Operational Security

PAA
Privileged Access Agreement

PAM
Pamphlet

PAO
Public Affairs Officer

PII
Personally Identifiable Information

PIT
Platform Information Technology

PKI
Public Key Infrastructure

PM
Program Manager

PPS
Ports, Protocols, and Services

RIG
Resources Integration Group

RMF
Risk Management Framework

SA
Special Access

SAP
Special Access Program

SCA
Security Control Assessor

SCI
Sensitive Compartmented Information

SIPRNet
Secure Internet Protocol Router Network

SP
Special Publication

SSE
Systems Security Engineering

STIG
Security Technical Implementation Guides

T&E
Test and Evaluation

TIG
The Inspector General

TPI
Two Person Integrity

USACIDC
U.S. Army Criminal Investigation Command

UCDMO
Unified Cross Domain Management Office

USC
United States Code

WMA
Warfighter Mission Area

Section II
Terms

Authenticator
The value or data object (e.g., a password, a biometric template, or a cryptographic key) used to prove the claimant possesses and controls the identity credential. Assertion based authenticators (e.g., a personal identity number, a password, or a passphrase) are data with no associated physical characteristics or device.
Cryptographic-based authenticators are cryptographically generated data or keys (usually only machine readable) carried or stored on a physical device such as the crypto module on a smartcard. Defined in DoDI 8520.03.

Acceptable Use
Outlines the acceptable use of computer equipment within a DoD/Army organization.

Authorizing Official
A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Defined in CNSSI 4009.

Authorized User
Any appropriately cleared individual required to access IT to carry out or assist in a lawful and authorized governmental function. Authorized users include: DoD employees, contractors, and guest researchers.

Capability
Defined in DoDI 8115.02.

Commercial Solutions for Classified
A commercial off-the-shelf (COTS) end-to-end strategy and process in which two or more COTS products can be combined into a solution to protect classified information.

Compilation
An aggregation of preexisting items of information. Pursuant to DoDM 5200.01-V1, compilations of information that are individually unclassified (or classified at a lower level) may be classified (or classified at a higher level) if the compiled information reveals an additional association or relationship that qualifies for classification and is not otherwise revealed by the individual elements of information.

Cryptographic High Value Product
NSA-approved products incorporating only UNCLASSIFIED components and UNCLASSIFIED cryptographic algorithms. This includes COTS, products approved by NSA, but does not include composed commercial solutions or their components, unless an individual component has been approved as a CHVP.
Un-keyed CHVPs are not classified or designated as controlled cryptographic item (CCI).

Cyber Attack
An attack, via cyberspace, targeting an enterprise use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Events
Any observable occurrence in a system and/or network.

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

Cybersecurity Architecture
Consists of strategies, standards, and plans that have been developed for achieving an assured, integrated, and survivable information enterprise. Defined in DoD Instruction 8510.01.

Cybersecurity Service Provider
Defined in DoD Directive 8530.1

Cybersecurity Workforce
Develops and maintains a trained and qualified cybersecurity workforce by providing a continuum of learning from basic literacy to advanced skills, recruiting and retaining highly qualified professionals, and keeping workforce capabilities current in the face of constant change.

Cyberspace
A global domain within the information environment.

Cyberspace Operations
The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Defined in JP 1-02.

DoD Information Network Operations
Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. Defined in JP 1-02.

Defensive Cyberspace Operations Defensive Internal Measures
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Defined in JP 1-02.

Electronic Communication
The transfer of information (signs, writing, images, sounds, or data) transmitted by computer, phone, or other electronic device. Electronic communication includes, but is not limited to: text messages, emails, chats, instant messaging, screensavers, blogs, social media sites, electronic device applications, and web/video conferencing.

Incident Response
Actions conducted to resolve information systems security incidents, restore systems to operational status, and provide technical and administrative corrections to protect systems from further attacks.

Information Owner
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. Defined in CNSSI 4009.

Information System Owner
Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information Technology
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition,

storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which— 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Information Technology Lifecycle
The IT lifecycle (e.g., concept definition, design and development, test and evaluation, procurement, installation, operation, maintenance, and disposal).

Insider Threat
The threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. Defined in DoDD 5205.16.

Intrusion
Unauthorized act of bypassing the security mechanisms of a system.

Key Management
The activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

Mission Partners
Those with whom DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, State and local governments, allies, coalition members, host nations and other nations, multinational organizations, non- governmental organizations, and the private sector. Defined in DoDD 8000.01.

Operating Environment
The environment in which users run application software.

Portfolio Management
The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability.

Principle of Least Functionality
Helps to minimize the potential for introduction of security vulnerabilities and includes, but is not limited to, disabling or uninstalling unused/unnecessary operating system (OS) functionality, protocols, ports, and services, and limiting the software that can be installed and the functionality of that software.

Principle of Least Privilege
Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of IT.

Risk Management Framework
Process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of Security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. (NIST Special Pub 800-53)

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Defined in CNSSI 4009.

Safeguard

Protection included to counteract a known or expected condition. Incorporated countermeasure or set of countermeasures within a base release.

Service Provider

An organization that provides one or more cybersecurity services to implement and protect the DoDIN.

Systemic Issue

Systemic issues normally include functional systems such as personnel and logistics and tend to surface through a general pattern of noncompliance throughout the various echelon of a command. The problem are often beyond the ability of local commanders to solve, so something may be wrong with the system.

User Activity Monitoring

The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing US Government information in order to detect insider threats and to support authorized investigations.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Defined in CNSSI 4009.

USAREC

ELECTRONIC PUBLISHING SYSTEM

DATE:	30 NOVEMBER 2017
DOCUMENT:	USAREC REG 25-2
SECURITY:	UNCLASSIFIED
DOC STATUS:	REVISION(Admin)