SECRETARY OF THE ARMY
WASHINGTON

14 OCT 2020

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2020-12 (Department of Defense Enterprise Email Trusted Agents)

1. References. For applicable references, see enclosure 1.

2. Purpose. This directive assigns responsibilities and prescribes procedures for the search of journaled Non-classified Internet Protocol Router Network (NIPRNET) Department of Defense Enterprise Email (DEE).

3. Applicability. This directive applies to the Regular Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve.

4. Policy.

a. The Chief Information Officer (CIO) is designated as the single Army Appointing Official for DEE Trusted Agents (TAs) to search journaled NIPRNET DEE. The CIO will—

(1) Appoint two primary TAs and two alternate TAs to conduct searches of NIPR journaled email for each nominating activity, following procedures prescribed in enclosure 2. Trusted agents will be, at minimum, in the grade of CPT/GS-12. A nominating official may nominate a CW3 if the nominating official certifies that the CW3 candidate possesses sufficient skills and experience to serve as a TA for the requesting activity. The appointing authority may be delegated to a military or civilian employee within the CIO organization or direct reporting unit at a minimum grade of COL/GS-15. Each activity may request CIO approval to increase or decrease its number of TAs based on workload. The following activities are responsible for nominating TAs to conduct searches, as needed, for the purposes indicated:

(a) Office of the Administrative Assistant to the Secretary of the Army—Freedom of Information Act (FOIA) requests, Privacy Act requests, records management, and purposes not assigned to another Army activity

(b) Office of the Deputy Chief of Staff, G-2—counterintelligence investigations

(c) Office of the Provost Marshal General and Criminal Investigation Command—criminal investigations

(d) U.S. Army Legal Services Agency—litigation, including reasonably anticipated litigation and litigation to which the Army is not a party, and eDiscovery

(2) When appropriate, appoint TAs at any other Army activity.

(3) Revoke appointments of TAs found to have committed misconduct.

b. Nominating officials from the activities listed in paragraph 4a(1) of this directive will take the following action:

(1) Follow procedures promulgated by the CIO to nominate TAs.

(2) In coordination with the Defense Information Systems Agency and the CIO, revoke system access of TAs found to have committed misconduct.

c. In addition to procedures and guidance provided by the CIO, TAs and activities requesting searches for NIPR journaled email will refer to Defense Information Systems Agency guidance described in enclosure 3. This guidance will be provided by the Army Appointing Official.

d. If a search yields relevant documents, TAs will notify, via email, the personnel whose accounts were searched, except in cases of counterintelligence investigations, criminal investigations, litigation, and eDiscovery.

5. Proponent. The Army CIO is the proponent for this policy and will incorporate the relevant provisions of this directive into Army Regulation 25–1 within 2 years of the date of this directive.

6. Duration. This directive will be rescinded on publication of the revised regulation.

Ryan D. McCarthy

Encls

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
(CONT)

DISTRIBUTION: (CONT)

- U.S. Army Materiel Command
- U.S. Army Futures Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command

Superintendent, U.S. Military Academy
Director, U.S. Army Acquisition Support Center
Superintendent, Arlington National Cemetery
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency

CF:
Director of Business Transformation
Commander, Eighth Army

REFERENCES

a. Defense Information Systems Agency (DISA), (DISA Office of the General Counsel's Department of Defense Enterprise Email (DEE) Search Guide), 6 July 2018 (or latest version)

b. DISA, DoD Enterprise Email (DEE) memorandum (Appointing Mission Partner Trusted Agents for Journaled/NIPR Email Searches), 19 March 2019

c. DISA (Department of Defense Enterprise Email (DEE) Tactics, Techniques, and Procedures: Requesting & Conducting a Legal Search and Hold of DEE Email), version 1.5.1, 19 March 2019 (or latest version)

d. Army Regulation (AR) 25–1 (Army Information Technology), 15 July 2019

e. AR 25–400–2 (The Army Records Information Management System (ARIMS)), 2 October 2007

f. AR 27–40 (Litigation), 19 September 1994

g. AR 380–67 (Personnel Security Program), 24 January 2014

h. Army General Orders 2020–01 (Assignment of Functions and Responsibilities Within Headquarters, Department of the Army), 6 March 2020

i. Administrative Assistant to the Secretary of the Army memorandum (Records Management and Email Use: Guidance for Senior Leaders), 8 March 2018

j. Chief Information Officer/G-6 memorandum (Enterprise Email Journaling), 11 November 2013

PROCEDURES TO NOMINATE AND APPOINT ARMY TRUSTED AGENTS TO SEARCH NIPR JOURNALED EMAILS

1. Background. Beginning 1 January 2020, the Army must appoint Trusted Agents (TAs) to access Army NIPR journaled email accounts.

2. Applicability. These procedures apply to the Chief Information Officer (CIO); Office of the Administrative Assistant to the Secretary of the Army; U.S. Army Legal Services Agency (USALSA); Office of the Provost Marshal General (OPMG); Criminal Investigation Command (CIDC); Deputy Chief of Staff, G-2; and activities identified in the future as requiring TAs.

3. Nomination procedure.

a. Effective immediately, principal officials (or those designated by the principal official) of activities identified in paragraph 4 of Army Directive 2020-12 (Department of Defense Enterprise Email Trusted Agents) will submit nominations of 2 primary and 2 alternate TAs by forwarding nominations to the Army Appointing Official for DEE TAs at usarmy.pentagon.hqda-cio-g-6.mbx.policy-inbox@mail.mil.

b. Nominations must include:

(1) two fully completed DD 2875 forms (System Authorization Access Request) signed by the nominee and the nominating official

(2) an unsigned, but otherwise complete, appointment memorandum (A sample memorandum is included in this enclosure.)

(Note: For additional guidance, see Defense Information Systems Agency (Department of Defense Enterprise Email (DEE) Tactics, Techniques, and Procedures: Requesting & Conducting a Legal Search and Hold of DEE Email), version 1.5.1, 19 March 2019 (or latest version).

c. TAs must be military or civilian employees with a minimum grade of CPT or GS-12. Nominees in the grade of CW3 will be considered if the nominating official certifies that the CW3 candidate possesses sufficient skills and experience to serve as a TA for the requesting activity. Supervisors may assign a military or civilian employee of lower rank/grade who demonstrates sufficient maturity and ability. TAs must be trustworthy and meet the following requirements:

(1) Comply with applicable laws, regulations, and policies for the release of official information, including the protection of privileged information, personally identifiable information, and other sensitive information.

(2) Successfully complete, within 30 days of appointment, the Records Management Training Course and Privacy Act Training in the Army Learning

Management System and provide certificates of completion of the training to the Appointing Official.

(3) Possess, at minimum, a favorable National Agency Check with Inquiries. In cases of data spillage, a TA must have clearance equal to the highest classification of data in the NIPR journaled DEE account.

(4) Have, in the judgement of the nominating official, sufficient computer skills and knowledge of the nominating activity's responsibilities that would require TAs to access Army NIPR journaled email accounts.

4. Appointment procedure. If requirements are met, the appointing official will approve the appointment in a signed memorandum sent via email to both the nominator and nominee. (A sample memorandum is included in this enclosure.)

5. Appointment revocation procedure. TAs are subject to appropriate disciplinary action for breaches of TA responsibilities under applicable laws and regulations. Should revocation of an appointment be necessary, the nominating official will submit to the Defense Information Systems Agency, as soon as practicable, two signed DD Forms 2875 (one for Out-of-Band Network and one for CommVault Console), copying the Appointing Official, to deactivate TA access to NIPR journaled emails. Revocation occurs when a TA resigns, retires, changes duties, changes position, or otherwise should no longer have TA access. The TA's access to the search request "email address" will also be revoked.

6. Recertification. Every 2 years, the nominating official will recertify to the appointing official, via email, that the TA still meets the requirements to serve in that capacity.

7. Sample appointment memorandum. To appoint a trusted agent, use the memorandum template that follows.

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer

SAIS-ZA [Date]

MEMORANDUM FOR [Trusted Agent], [Activity] [Office Symbol], [Address]

SUBJECT: Appointment of Trusted Agent

1. Effective [Day Month Year], [Appointee], [Appointee Position], [Appointee Organization], [Appointee Phone], [Appointee Email], is appointed as an Army Trusted Agent (TA) to search NIPR journaled emails.

2. Authority: Army Directive 2020-12 (Department of Defense Enterprise Email Trusted Agents).

3. As a Trusted Agent, you may be subject to appropriate disciplinary actions for breaches of your TA responsibilities pursuant to applicable laws and regulations. You must meet these requirements:

a. Comply with applicable laws, regulations, and policies for the release of official information, including the protection of privileged information, personally identifiable information, and other sensitive information.

b. Possess a valid security clearance.

c. Complete the Records Management Training Course and Privacy Act Training in the Army Learning Management System within 30 days of appointment.

d. Follow procedures described in these references:

(1) Defense Information Systems Agency (Office of the General Counsel's Department of Defense Enterprise Email (DEE) Search Guide), 6 July 2018 (or latest version)

(2) Defense Information Systems Agency (Department of Defense Enterprise Email (DEE) Tactics, Techniques, and Procedures: Requesting & Conducting a Legal Search and Hold of DEE Email), version 1.5.1, 19 March 2019 (or latest version)

(3) Army Directive 2020-12 (Department of Defense Enterprise Email Trusted Agents), 14 October 2020

e. Maintain logs of all requests received or processed. Logs must record each request by unique tracking number. Logs will include date and time of access, name(s) of any user accounts identified to be searched, the query search terms, the office initiating the search ("requesting activity"), the official submitting the access request, and the type of access request (such as criminal investigation, counterintelligence, administrative investigation, litigation, FOIA, or Privacy Act). The logs will be subject to review and inspection at any time by designated officials.

4. Period: until cancelled.

5. Cancellation. I retain the authority to cancel or withdraw this appointment at any time. The appointment is cancelled by your resignation, retirement, change of duties, or change of position.

[Signature Block of
CIO or Designated
Appointing Official]

PROCEDURES FOR REQUESTING SEARCHES OF NIPR JOURNALED EMAILS AND RECORDKEEPING REQUIREMENTS

1. References.

a. Defense Information Systems Agency (DISA), (DISA Office of the General Counsel's Department of Defense Enterprise Email (DEE) Search Guide), 6 July 2018

b. DISA, (Department of Defense Enterprise Email (DEE) Tactics, Techniques, and Procedures: Requesting & Conducting a Legal Search and Hold of DEE Email), version 1.5.1, 19 March 2019

2. Search initiation procedure. The search request process begins when a requesting activity identifies a need to access NIPR journaled email accounts hosted and stored electronically on the DEE or receives a request from another organization or person for a search of a NIPR journaled email account. For detailed guidance, see references 1a and 1b.

3. Legal review and approval. All Army individuals and activities requesting a search of NIPR journaled email are responsible for obtaining the legal reviews or approvals required by their command.

4. Search requests. See reference 1a for details on documentation required for search requests. Failure to include such documentation will delay processing. Send search requests, including all required documentation, to the following email addresses:

a. Office of the Administrative Assistant. Email search requests under the purview of the Office of the Administrative Assistant to the Secretary of the Army (Freedom of Information Act, Privacy Act, records management, and any other purpose not assigned to another Army activity) to usarmy.pentagon.hqda-cio-g-6.mbx.NIPR-Journaled-DEE-Search-FOIA@mail.mil. Emails must be encrypted and digitally signed.

b. Deputy Chief of Staff, G-2 (DCS, G-2). Email search requests under the purview of DCS, G-2 (counterintelligence investigations) to usarmy.pentagon.hqda-cio-g-6.mbx.NIPR-Journaled-DEE-Search-CIA@mail.mil. Emails must be encrypted and digitally signed.

c. Office of the Provost Marshal General (OPMG) and Criminal Investigation Command (CIDC). Email search requests under the purview of OPMG and CIDC (criminal investigations) to usarmy.pentagon.hqda-cio-g-6.mbx.NIPR-Journaled-DEE-Search-Inv@mail.mil. Emails must be encrypted and digitally signed.

d. United States Army Legal Services Agency (USALSA). Email search requests under the purview of USALSA (litigation, including reasonably anticipated litigation and litigation to which the Army is not a party, and eDiscovery) to

usarmy.pentagon.hqda-cio-g-6.mbx.NIPR-Journaled-DEE-Search-Lit@mail.mil. Emails must be encrypted and digitally signed.

5. NIPR journaled email search recordkeeping requirements. Trusted Agents will provide the following information in the Army Records Information Management System:

a. Title: Trusted Agent—access and disclosure request files

b. Description: appointed individuals authorized to search senior Army officials' emails captured and maintained for case files created in response to requests for information, such as eDiscovery, Freedom of Information Act, Privacy Act, Mandatory Declassification Review, and similar access programs

c. Disposition: KE6—event is after appointment revocation. Keep in Central Filing Area until no longer needed for conducting official business, then retire/upload to the Army Electronic Archive (AEA). The AEA will destroy 6 years after event occurs. Request for longer retention may be authorized by the United States Army Records Management and Declassification Agency if required to conduct official business.

d. Disposition Authority: GRS 4.2—item 20 (DAA-GRS2016-00020001).