



# Defense Health Agency **ADMINISTRATIVE INSTRUCTION**

**NUMBER 097**  
September 06, 2018

---

---

J-1/ISD

**SUBJECT:** Insider Threat Program

**References:** See Enclosure 1.

1. **PURPOSE.** This Defense Health Agency-Administrative Instruction (DHA-AI), based on the authority of References (a) through (c), and in accordance with the guidance of References (d) through (u), establishes the Defense Health Agency's (DHA) procedures to:

a. Develop, coordinate, and implement an Insider Threat Program across the DHA. This program is to deter, detect, prevent, respond to, and mitigate against unintentional or intentional incidents which could harm individuals, lead to unauthorized disclosure of information, and/or damage government property and resources.

b. Maintain a fusion and analysis center, hereafter referred to as the Hub, tasked with the integration of insider threat detection capabilities and analysis of insider threat indicators across the DHA.

c. Maintain an Insider Threat Working Group (ITWG) to ensure that the appropriate mechanisms are in place to provide relevant insider threat information to the Hub. The ITWG will be required to provide subject matter expertise regarding insider threat mitigation strategies during the referral process.

2. **APPLICABILITY.** This DHA-AI applies to all DHA personnel to include: assigned, attached, or detailed Service members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary or permanent duties at DHA, to include intermediate management organizations, markets, and Medical Treatment Facilities (MTFs).

3. POLICY IMPLEMENTATION. It is DHA's policy, pursuant to References (d) through (p), that:

a. A Hub will be established to perform assessments and analysis on reported potential insider threat indicators. Hub analysts will ensure that all information (e.g., documents, files, and any other material provided to the Hub) is protected in accordance with this DHA-AI, References (n) through (u), and approved Hub procedures.

b. Hub analysts and ITWG members will be required to sign Non-Disclosure Agreements prior to gaining access to any information or material related to insider threat inquiries or Hub operations.

c. All DHA program offices will support the Insider Threat Program by securely providing the Hub with regular or event-driven notifications and/or responses to specific requests for information including, but not limited to:

- (1) Personnel security;
- (2) Physical security;
- (3) Information security;
- (4) Law enforcement;
- (5) Counterintelligence (CI);
- (6) User Activity Monitoring (UAM);
- (7) Cybersecurity;
- (8) Legal; and

(9) Other data sources the Insider Threat Program Manager (PM) considers necessary and appropriate.

d. DHA personnel will report to the Hub in times of possible insider threats and any other activity indicative of a threat to DHA personnel and/or resources. A list of potential indicators and activities used to detect a potential insider threat is listed in Enclosure 4.


4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. **RELEASABILITY. Not cleared for public release.** This DHA-AI is available to users with Common Access Card authorization on the DHA SharePoint site at: <https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx>.

7. **EFFECTIVE DATE.** This DHA-AI:

- a. Is effective upon signature.
- b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with DHA-Procedural Instruction 5025.01 (Reference (c)).



R. C. BONO  
VADM, MC, USN  
Director

Enclosures

1. References
2. Responsibilities
3. Procedures
4. Potential Indicators

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
- (b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
- (c) DHA-Procedural Instruction 5025.01, "Publication System," August 21, 2015, as amended
- (d) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended
- (e) DoD Instruction 1438.06, "DoD Workplace Violence Prevention and Response Policy," January 16, 2014
- (f) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended
- (g) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
- (h) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
- (i) DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012, as amended
- (j) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- (k) United States Code, Title 5, Section 552a
- (l) DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016
- (m) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 1, 2003
- (n) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Healthcare Programs," August 12, 2015
- (o) DHA Insider Threat Working Group (ITWG) Charter, February 5, 2016<sup>1</sup>
- (p) United States Code 3381, Title 50, Section (e)
- (q) Code of Federal Regulations, Title 5, Part 1209
- (r) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (s) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
- (t) Public Law 83-703, "Atomic Energy Act of 1954," June 2005, as amended
- (u) DHA-Administrative Instruction 088, "Office of Inspector General (OIG)," February 28, 2017

---

<sup>1</sup>The signed DHA ITWG Charter is available upon request. Requests can be made to the DHA Insider Threat PM.

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will:

a. Implement the minimum standards and requirements for Executive Branch Insider Threat Programs listed in References (d) and (e).

b. Appoint a Senior Official (SO) to provide management, accountability, and oversight of the Insider Threat Program.

c. Provide required reports and requested information to the Under Secretary of Defense for Intelligence.

d. Provide required input to the DoD Chief Information Officer.

2. OFFICE OF INSPECTOR GENERAL (OIG), DHA. In addition to the responsibilities of the Deputy Assistant Directors (DADs), OIG, DHA, may conduct reviews at the request of the Insider Threat PM, of the Insider Threat Program, to ensure compliance with insider threat policy guidelines and legal, privacy, and civil liberty protections as listed in References (i) through (n). The reviews will be conducted independently of the ITWG OIG Working Group members.

3. DADs, DHA. The DADs, DHA, will:

a. Provide a representative (e.g., a core voting member) to the ITWG.

b. Promptly provide owned, or managed information on DHA personnel to the Hub, upon request, or when potential indicators are discovered.

c. Assist in the development of Insider Threat Program requirements, doctrine, and identification of emerging capabilities, as well as tactics, techniques, and procedures to counter insider threats.

d. Incorporate insider threat requirements into planning, programming, and budgeting, as applicable, to support the Insider Threat Program.

e. Facilitate independent, third-party assessments of the Insider Threat Program.

f. Complete the essential tasks set forth in the implementation plan developed by ITWG.

4. DAD, INFORMATION OPERATIONS (IO) (J-6). In addition to the responsibilities of the other DADs, the DAD, IO (J-6), will:

- a. Implement UAM of DHA enclaves for the DoD Insider Threat Program, in accordance with Reference (f).
- b. Implement and audit UAM standards, network security, operational performance, compliance, configuration control, and assessment and authorization of DHA enclaves, in accordance with References (g) and (h).
- c. Provide owned, or managed, information on DHA personnel to the Hub, upon request, or when potential indicators are discovered.
- d. Conduct periodic evaluation and reviews, at least annually, of the insider threat mission area and cyber capability and capacity seams, gaps, and resource planning. Results of evaluations are reported in accordance with Reference (d).
- e. Provide resource and acquisition guidance necessary for Insider Threat Program wholeness and effectiveness. This includes, but is not limited to, advocating for cybersecurity resources to support the Insider Threat Program directly or, indirectly, through cybersecurity programs.

5. MTFs. The MTFs will:

- a. Establish, provide oversight, and manage an Intermediate Management Organization-level Insider Threat Program for all associated MTFs (e.g., hospitals, clinics, and centers).
- b. Report all potential or actual concerns to the DHA enterprise-level insider threat Hub.
- c. Develop and promulgate Insider Threat Program procedures in accordance with the references in Enclosure 1.

6. SO, INSIDER THREAT PROGRAM. The SO, Insider Threat Program, will report any insider threat inquiry or indicator, deemed to pose an imminent or significant threat to DHA personnel or resources, directly to the Chief of Staff, DHA. To execute the above, the SO will:

- a. Perform his/her duties in accordance with References (d), (e), and (q).
- b. Establish, provide oversight, and manage the Insider Threat Program across all mission areas, programs, activities, processes, and procedures.
- c. Ensure program assessments are conducted to ensure compliance with national and DoD insider threat requirements to gauge effectiveness and efficiency of the Insider Threat Program.

- d. Establish and exercise operational control of a DHA enterprise-level insider threat Hub to integrate and manage insider threat information.
- e. Provide oversight and leadership for the ITWG. Annually review the program requirements set forth in Reference (o), for currency and relevance.
- f. Appoint an Insider Threat PM.
- g. Ensure that the Insider Threat Program is adequately resourced and ready for execution.
- h. Coordinate with the appropriate offices on matters concerning “whistleblowers,” in accordance with Reference (q).
- i. Establish guidance governing the specific information provided to the Hub for analysis.
- j. Ensure the Hub has timely access to available U.S. Government Intelligence and CI reporting information and analytic products pertaining to adversarial threats.
- k. Ensure the establishment of guidelines for the protection and privacy of Insider Threat Program files.
- l. Provide an annual report to the Director, DHA, documenting program accomplishments, allocated resources, agency risk(s), program improvement goals, and documented challenges.
- m. Provide oversight for the integration of activities with other DoD Insider Threat Programs.
- n. Ensure that DHA representative(s) attend DoD and interagency forums engaged in countering insider threats.
- o. Develop and promulgate Insider Threat Program requirements and an implementation plan, in accordance with References (d) and (e).
- p. Ensure standardized processes and procedures are in place to allow the Hub to centrally gather, integrate, analyze, and provide resolution strategies to the SO regarding inquiries of potential indicators of an insider threat.
- q. Develop and promulgate a Memorandum of Agreement to establish the framework and set forth the terms, responsibilities, and procedures for sharing investigative, security clearance, and other relevant information between the Naval Criminal Investigative Service and the Hub.

7. INSIDER THREAT PM. The Insider Threat PM will:

- a. Report directly to the SO on insider threat-related matters.

- b. Manage daily operations of the Hub.
- c. Chair and facilitate ITWG meetings.
- d. Provide required insider threat awareness training, and ensure that all DHA personnel complete the training annually. Hub personnel may require additional training in accordance with this DHA-AI and Reference (q).
- e. Proactively identify and protect DHA personnel with whistleblower status from unauthorized monitoring in accordance with Reference (q).
- f. In association with the DAD, IO (J-6), identify, implement, and maintain an effective insider threat auditing and analysis software package for DHA computer systems, and coordinate with the Defense Information Systems Agency and other external agencies, as appropriate.
- g. Establish management controls for the Hub to include proper procedures for the handling and utilization of files and other data provided by DHA personnel or directorates.
- h. Ensure access to records and data is restricted to Insider Threat Program personnel with the proper clearance and a need-to-know basis. Records will be kept permanently until National Archives and Records Administration publishes retention and destruction guidelines for unclassified and classified information.
- i. Facilitate program reviews to ensure compliance with DoD's Insider Threat Policy and Program guidelines.
- j. Complete the essential tasks set forth in the implementation plan.
- k. Coordinate efforts with the DoD Insider Threat Management Analysis Center and National Insider Threat Task Force as required.

8. ADVISORY MEMBERS. In accordance with Reference (o), the Advisory Members will:

- a. Provide ad hoc support to the ITWG, upon request, by the SO or PM.
- b. Identify and provide the Hub access to information, as authorized, consistent with References (d) and (e).
- c. Provide certified medical and psychological expertise to the Insider Threat Program including, without limitation, advice pertaining to clinical issues relevant to the behaviors observed, and mitigation of potential insider threat activities in coordination and communication with the Hub consistent with applicable laws, policies, regulations, and orders.



d. Assist in the development of Insider Threat Program policy, doctrine, and identification of emerging capabilities, as well as tactics, techniques, and procedures.

e. Incorporate insider threat requirements into planning, programming, and budgeting, as applicable, to support the Insider Threat Program.

f. Facilitate independent assessments of the implementation of the Insider Threat Program.

g. Assist in the completion of the essential tasks set forth in the implementation plan.

9. DHA PERSONNEL. DHA personnel will be trained to recognize and report potential insider threat and work place violence indicators, as well as potential terrorism activity. They will also be provided information regarding referrals to the Hub. DHA personnel will:

a. Immediately report imminent threats to law enforcement and security personnel.

b. Attend initial and annual training sessions on insider threat and workplace violence prevention.

c. Refer fellow employees to the Hub, if potential indicators are recognized.

d. Assist the Hub in obtaining additional available information, as required.

e. Assist Hub personnel in making further determinations regarding employee actions that may cause harm to DHA personnel, property, or information.

ENCLOSURE 3

PROCEDURES

1. REPORTING. Insider threat indicators must be reported directly to the Hub within one (1) hour of the occurrence. Unclassified reports may be provided directly to the Hub via phone at (703) 681-6777, or e-mail at dha.insider-threat@mail.mil. For classified reports, provide an initial notification via phone at (703) 681-6777, and send the detailed information via email to dha.insider-threat@mail.smil.mil.

2. TRAINING. The Insider Threat Awareness training will:

a. Be provided in person to all DHA employees within 30 days of initial employment.

b. Be completed through instructor-led or computer-based training for mandatory annual refresher training.

c. Address current and potential threats in the work and personal environment and include, at a minimum, the following topics:

(1) The importance of detecting insider threats;

(2) The importance of reporting suspicious activity to insider threat personnel;

(3) How to report suspicious activities and insider threat indicators;

(4) Methodologies of adversaries to recruit trusted insiders and collect information; and

(5) CI and security reporting requirements.

3. POTENTIAL INDICATORS. The behaviors and indicators of potential or actual insider threats vary depending on the scenario. The Insider Threat Program will utilize both technology and human observance techniques to ensure that all potential and actual concerns are thoroughly analyzed. Enclosure 4 contains a list of potential indicators of insider threat activities for personnel with access to classified or sensitive information, as well as potential indicators for personnel that may be involved with terrorism or contemplating work place violence.

4. HUB ORGANIZATION AND FUNCTIONS. The Hub will act as the fusion and analysis center for all insider threat information and reporting.

a. The Hub's assigned personnel will be comprised of government, military, and/or contract support personnel from the DHA Mission Assurance Branch.

b. Personnel assigned to the Hub will implement the Insider Threat Program through:

(1) Managing, standardizing, focusing, and aligning the Insider Threat Program to comply with References (d) through (s).

(2) Coordinating information sharing and Memorandums of Agreement, as necessary, with supporting security agencies to counter insider threats.

(3) Functioning as the central analytical entity tasked to gather, analyze, report, and provide recommendations to senior leadership regarding insider threat-related information (e.g., active shooter, workplace violence, workplace harassment, espionage, sabotage, and acts of terrorism with an insider nexus across the DHA).

(4) Coordinating with the DAD, IO (J-6), to establish and manage user auditing and monitoring tools on all DHA networks, in accordance with References (f) through (h).

(5) Training employees on insider threat awareness and reporting responsibilities. To include coordination with Human Resources Division and the Learning and Development Division to ensure insider threat awareness training is part of in-processing for new employees, and included on the DHA Training Database to facilitate the completion of annual refresher training.

(6) Compliance with civil liberties and privacy laws, in accordance with References (i) through (n).

(7) Compliance with whistleblower protections, in accordance with Reference (q).

(8) Establishing and maintaining information on internal networks to promote the Insider Threat Program, and providing DHA employees with insider threat information, reference materials, and reporting procedures.

(9) Providing DHA employees a secure, anonymous, and electronic mean(s) of reporting insider threat indicators to the Hub.

c. Detailed procedures, upon receipt of the initial report, will be outlined in the Hub's Standard Operating Procedure, as approved by the SO. However, the Standard Operating Procedure will not be available for general distribution. The general procedures of the Hub, upon receiving a report, are as follows:

(1) The Hub will assess all initial reports of possible insider threat indicators and will coordinate appropriately with relevant ITWG members.

(2) When anomalies or threat information satisfies the criteria threshold needed to initiate an inquiry, the PM will brief the SO and request authorization to begin an active inquiry.

(3) Based on the information gathered, the Hub may recommend the inquiry be

internally resolved, placed into an internal repository, closed with no further action, or referred to a particular DHA Directorate, local law enforcement entity, the appropriate Military Department CI organization, or the Federal Bureau of Investigation, in accordance with References (d) and (p).

(4) The Hub's recommendation will be presented to the SO for a final determination.

5. ITWG AND FUNCTIONS. Per Reference (o), the DHA ITWG is chartered as the primary body to establish and implement the Insider Threat Program for the Agency. See Reference (o) for the functions, required actions, and membership of the ITWG.

6. PRIVACY AND CIVIL LIBERTIES. The protection of Privacy and Civil Liberties is a governing principle of the Insider Threat Program. Insider threat information, determined to be Controlled Unclassified Information, personally identifiable information, and/or protected health information, will be afforded all mandated protective measures, as outlined in References (i) through (n), (r) and (s).

7. WHISTLEBLOWER PROTECTION. Employees who make, prepare to make, or are perceived as making, or preparing to make a protected communication, termed a "whistleblower," will be afforded protection, in accordance with References (q) and (u).

ENCLOSURE 4

POTENTIAL INDICATORS

1. Preventing insider threat and workplace violence requires recognition of potential indicators and confidence that concerns can be reported and handled appropriately.

2. Tables 1 and 2 are not complete and do not serve as checklists, but they do provide possible behaviors and activities that should be reported if an individual exhibits actions that cause for concern. The following behaviors may indicate concerns that require reporting to the Hub. **Note:** These behaviors may be executed independently, in combination of, or may not be included in the table.

Table 1. Potential Insider Threat Indicators with Access to Classified or Sensitive Information

1.	When not related to official duties, contact with persons known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against facilities, organizations, personnel, or information systems. This includes contact through social events or social networking sites.
2.	Attempts by personnel to obtain or acquire unauthorized access to classified or sensitive information through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence), or automated system(s) intrusions or searches.
3.	Unauthorized contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
4.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
5.	Permitting others to acquire unauthorized access to classified or sensitive information systems.
6.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
7.	Removing or sending classified or sensitive material out of secured areas without proper authorization.
8.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
9.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
10.	Unwarranted work with classified/sensitive materials outside of normal duty hours.
11.	Attempts to place personnel or contractors under obligation through special treatment, favors, gifts, or money.

12.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
13.	Travel to foreign countries that are: <ol style="list-style-type: none"> <li>a. Short trips inconsistent with logical vacation travel and not part of official duties;</li> <li>b. Personal trips inconsistent with an individual's financial ability; and/or</li> <li>c. Concealed or done under false pretense.</li> </ol>
14.	Personnel who fail to report or are in repeated contact with any official or citizen of a foreign country when the foreign official or citizen: <ol style="list-style-type: none"> <li>a. Exhibits excessive knowledge of or undue interest in personnel or their government duties beyond the normal scope of friendly conversation;</li> <li>b. Attempts to obtain classified or national security sensitive information;</li> <li>c. Attempts to place personnel under obligation through special treatment, favors, gifts, money, or other means; and/or</li> <li>d. Attempts to establish business relationships that are improper or outside the scope of normal official duties.</li> </ol>
15.	Unexplained or undue affluence indicated by expenditures that an individual's income does not logically support.
16.	Behavior which calls into question or raises doubts about the individual's loyalty to the United States to include conduct which suggests possible involvement in espionage, terrorism, sabotage, or subversion.
17.	Personnel repeatedly unwilling to comply with rules and regulations, or to cooperate with information security requirements.
18.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of U.S. Government information.
19.	Unauthorized password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
20.	Use of another person's account credentials.
21.	Tampering with or introducing unauthorized elements into information systems.
22.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
23.	Downloading or installing non-approved computer applications on government systems.
24.	Unauthorized e-mail traffic to foreign destinations.
25.	Conducting denial of service attacks or suspicious network communications failures.
26.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
27.	Unexplained storage of encrypted data.
28.	Unauthorized use of multiple user or administrator accounts.
29.	Hacking or cracking activities.
30.	Social engineering, electronic elicitation, e-mail spoofing, or spear phishing.

31.	Introduction of malicious code or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data ex-filtration.
32.	Use of unauthorized scripts to detect and move data and files.
33.	Unauthorized manipulation of information in paper or electronic files.

Table 2. Indicators of Potential Terrorism Activity or Work Place Violence

1.	Advocating violence, the threat of violence, or the use of force to achieve goals either personally or on behalf of a known or suspected terrorist organization.
2.	Advocating support for a known or suspected terrorist organization or objective.
3.	Providing financial or other material support to a known or suspected terrorist organization or to someone suspected of being a terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives.
5.	Contact, association, or connections to known or suspected terrorists, including online, e-mail, and social networking contacts.
6.	Any attempt to contact personnel on behalf of a known or suspected terrorist organization or for terrorist activities.
7.	Collecting intelligence, including information regarding sensitive facility security procedures and capabilities for an unknown or unauthorized purpose.
8.	Family ties, or other close associations, to known or suspected terrorists or terrorist supporters.
9.	Repeated browsing or visiting known or suspected terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote terrorism or terrorist themes, without official sanction in the performance of duty.
10.	Possessing unauthorized weapons in the work place.
11.	Threatening to kill or harm supervisors, co-workers, or anyone else within or outside of the work place.
12.	Sending e-mails or posting on social media sites threatening communications against supervisors, co-workers, or anyone else within or outside of the work place.
13.	Increase in unsolicited comments about firearms, other dangerous weapons, and violent crimes.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CI	counterintelligence
DAD	Deputy Assistant Director
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
IO	Information Operations
ITWG	Insider Threat Working Group
MTF	Medical Treatment Facility
OIG	Office of Inspector General
PM	Program Manager
SO	Senior Official
UAM	User Activity Monitoring

PART II. DEFINITIONS

Controlled Unclassified Information. Unclassified information that requires safeguarding or dissemination controls as pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under References (n) and (p).

Hub. A fusion and analysis center tasked with the integration of insider threat detection capabilities and analysis of insider threat indicators.

insider. Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.

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.

MTF. Any fixed facility established for the purpose of furnishing medical and/or dental care to eligible beneficiaries, including all operations and all health care delivery associated with each such facility, and is funded by the Defense Health Program.



personally identifiable information. Information which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual.

protected health information. Individually identifiable health information that relates to the individual's past, present, or future physical or mental health, the provision of health care, or the payment for health services, and that identifies the individual or it is reasonable to believe the information can be used to identify the individual.

UAM. The capability to electronically monitor and track end user behavior on devices, networks, and other Information Technology resources and evaluate anomalous activity.

whistleblower. A person making a protected disclosure, that is a disclosure of information by an employee, former employee, or applicant that the individual reasonably believes evidences a violation of law, rule, or regulation, gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific danger to public health or safety. It does not include a disclosure that is specifically prohibited by law or required by Executive Order to be kept secret in the interest of national defense or foreign affairs, unless such information is disclosed to the Special Counsel, the Inspector General of an agency, or an employee designated by the head of the agency to receive it.

workplace violence. Any act of physical violence against persons or property, physical or verbal threats, intimidation, harassment, or other inappropriate, disruptive behavior that causes fear for personal safety at or outside of the work site.