DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5500.35
DUSN
22 Feb 2022

SECNAV INSTRUCTION 5500.35

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY PHYSICAL SECURITY PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Responsibilities
(3) Physical Security Standards
(4) Installation Access Control
(5) Deviations, Waivers, and Exceptions
(6) Arms, Ammunition, and Explosives (AA&E)
(7) Acronyms
(8) Definitions

1. Purpose. This instruction establishes the Department of the Navy (DON) Physical Security Program (PSP) per references (a) through (al), promulgates policy, assigns responsibilities, and mandates minimum physical security requirements.

2. Applicability. This instruction applies to all personnel employed by, detailed, or assigned to the DON, including civil servants, members of the active and reserve units of the United States Marine Corps and United States Navy; experts or consultants performing services for the DON through a personnel appointment or a contractual arrangement; industrial or commercial contractors, licensees, certificate holders, or grantees, including subcontractors; the DON Field Activities, and all other organizational entities in the DON (hereinafter referred to collectively as the "DON Components"). This instruction provides minimum standards for the protection of resources normally found on installations, afloat, and in expeditionary environments. This instruction is not applicable to the protection of:

a. Sensitive Compartmented Information Facilities.

b. Protection of Biological Select Agents and Toxins.

c. Security of Chemical Agents.

d. Security Policy for Protecting Nuclear Weapons.

e. Nuclear Reactors and Materials.

f. Nuclear Command and Control Facilities.

3. Policy. It is DON policy that:

a. The DON Services will promulgate physical security policy to ashore, afloat, and expeditionary units on and off installations, to include but not limited to, installations, facilities, sites, field activities, and vessels (ships, aircraft, etc.).

b. The DON Components will maintain a PSP to ensure the appropriate application of physical security policy and measures with the goal of protecting DON assets against all hazards and threats per references (a), (b), and this instruction. This protection:

(1) Will not be exercised in an arbitrary, unpredictable, or discriminatory manner. Personnel removal or denial actions must be based on reasonable grounds and be judiciously applied.

(2) Consistent with reference (c), will prohibit individuals from entering DON-controlled installations, sites, or facilities after they have been removed and ordered not to enter. If this order is violated, civilian offenders not subject to military law may be detained by the commander or civilian director of a DON installation or facility and may be subject to prosecution under federal, state, or local statutes.

c. The DON PSP is that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, resources, installations, facilities, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

d. DON PSPs are designed to prevent loss and reduce crime throughout the DON community and to provide a means to minimize threats when physical security measures are ignored or bypassed by others with or without ill intent.

e. PSPs employ protective measures and security procedures in combination with active or passive systems, technologies, devices, and security forces used to protect personnel, resources, installations, facilities and information from possible threats.

4. Responsibilities. See enclosure (2).

5. Physical Security Standards. See enclosure (3).

6. Installation Access Control. See enclosure (4).

7. Deviations, Waivers, and Exceptions. See enclosure (5).

8. Arms, Ammunition, and Explosives (AA&E). See enclosure (6).

9. Abbreviations and Acronyms. See enclosure (7).

10. Definitions. See enclosure (8).

11. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Office, the Office of the Chief of Naval Operations Records Manager, or the DRMD program office.

12. Information Management Control. The reporting requirements contained in:

a. Enclosure (2), paragraph 3h is exempt from information collection control, in accordance with reference (a1), Part IV, paragraph 7k.

b. Enclosure (3), paragraphs 7f, 8, and 9 are exempt from information collection control in accordance with reference (a1), Part IV, paragraphs 7n and 7o.

c. Enclosure (4), paragraphs 2b, 8b, and 10 are exempt from information collection control in accordance with reference (al), Part IV, paragraph 7n.

d. Enclosure (5), paragraph 2 is exempt from information collection control in accordance with reference (al), Part IV, paragraph 7n.

e. Enclosure (6), paragraph 2c is exempt from information collection control in accordance with reference (al), Part IV, paragraph 7n.

f. Enclosure (7), paragraph 2, is exempt from information collection control in accordance with reference (al), Part IV, paragraph 7n.

13. Forms. SECNAV 5512/1, Department of the Navy Local Population ID Card/Base Access Pass Registration is available on the official DON Issuances website: https://www.secnav.navy.mil/doni/default.aspx.

CARLOS DEL TORO

Distribution:
Electronic only, via Department of the Navy Issuances Website https://www.secnav.navy.mil/doni/.

REFERENCES

(a) DoD Instruction 5200.08 of 20 November 2015
(b) DoD 5200.08-R of 19 October 2020
(c) DoD Manual 5200.08 Volume 3, Physical Security Program: Access to DoD Installations of 2 January 2019
(d) SECNAVINST 5430.7S
(e) 10 U.S.C. §8013
(f) DoD Directive 5143.01 of 6 April 2020
(g) DoD Instruction 2000.16 Volume 1 of 20 November 2019
(h) DoD Instruction 2000.16 Volume 2 of 8 May 2017
(i) SECNAVINST 3300.2C
(j) SECNAVINST 3501.1D
(k) SECNAVINST 5500.37
(l) DoD Directive 5200.43 of 14 July 2020
(m) SECNAVINST 5500.36A
(n) DoD Instruction 3224.03 of 4 June 2020
(o) DoD Instruction 8510.01 of 28 July 2017
(p) DoD Manual 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information of 28 July 2020
(q) DoD Directive 8521.01E of 15 October 2018
(r) DoD Instruction 8500.01 of 7 October 2019
(s) DoD Instruction 5400.11 of 29 January 2019
(t) DoD Instruction 6055.17 of 12 June 2019
(u) DoD Directive 5210.56 of 18 November 2016
(v) DoD Instruction 5100.76 of 19 October 2020
(w) DoD Manual 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E) of 5 October 2020
(x) DoD Memorandum “Installation Security and Unauthorized Installation Access” of 4 April 2019
(y) SECNAVINST 5530.4E
(z) DoD Manual 4140.01, Volume 5, of 17 September 2018
(aa) DoD Instruction 6055.16 of 31 August 2018
(ab) 50 U.S.C. §797
(ac) DoD Directive 5230.20 of 22 June 2005
(ad) DoD Instruction 5525.19 of 1 October 2020
(ae) 18 U.S.C. §499
(af) SECNAVINST 5430.107A
(ag) DoD Directive 6055.09E of 26 June 2019
(ah) DTR 4500.9-R
(ai) DoD Instruction 6055.07 of 31 August 2018

(aj) DoD 4145.26-M, DoD Contractors Safety Manual for Ammunition and Explosives of 31 August 2018
(ak) DoD Instruction 4140.01 of 6 March 2019
(al) SECNAV M-5214.1

RESPONSIBILITIES

1. The Under Secretary of the Navy (UNSECNAV) is designated as the deputy and principal assistant to the Secretary of the Navy (SECNAV), and oversees the implementation of the DON physical security program in his role as Chief Operating Officer, with the advice and assistance of the Deputy Under Secretary of the Navy (Intelligence and Security) (DUSN (I&S)), as designated in reference (d).

2. Deputy Under Secretary of the Navy (Intelligence and Security)(DUSN I&S). The DUSN (I&S) will:

a. Oversee and establish policy and provide guidance for the administration and management of an effective and efficient DON PSP.

b. Consistent with reference (e), represent the SECNAV during the coordination of Executive Orders, Department of Defense (DoD), and DON policy issuances, including physical security directives, policies, and procedures established for the protection of DON installations, facilities, personnel, and assets.

c. Senior Director for Intelligence & Security (SDI&S). The SDI&S will:

(1) Develop and improve DON instructions, consistent with reference (b), to guide and direct DON PSP activities. Coordinate, as appropriate, with other DON principal staff assistants when developing physical security policy and programs directly affecting their areas of assigned responsibilities.

(2) Ensure standardized security equipment and processes are implemented, to the maximum extent possible and with appropriate provisions for unique missions and security environments, to ensure maximum interoperability, consistent quality assurance, and cost savings.

(3) Ensure physical security investments are guided by a capital planning and investment control process that is risk-based and informs the Department’s planning, programming, budgeting, and execution processes.

(4) Coordinate with key stakeholders on physical security matters that affect DON antiterrorism planning and critical assets in accordance with references (g) through (j) and this instruction.

(5) Coordinate with key stakeholders on physical security matters that affect DON counterintelligence planning in accordance with reference (b).

(6) Establish and manage the DON Physical Security Working Group (PSWG). The DON PSWG will evaluate and analyze the concepts, management systems, policy, doctrine, security programs, and supporting materiel systems for physical security within the DON.

(a) The DON PSWG will be chaired by a DUSN representative at the O6/GS15 level and will be supported by the DON Services at a commensurate level.

(b) The DON PSWG will meet semi-annually at a minimum, and more frequently, as required by emerging issues. The DON PSWG may be combined with other DON level working groups stood up pursuant to reference (n).

(7) Coordinate with the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) and the Assistant Secretary of the Navy for Energy Installations & Environment (ASN (EI&E)) to develop and establish physical security standards to include design, procurement, deployment, installation, integration, technology refreshment, and life cycle sustainment (i.e. Electronic Security Systems (ESS), Intrusion Detection Systems (IDS), Active Vehicle Barriers (AVB), etc.).

(8) Report all approved physical security deviations to the Office of the Secretary of Defense (OSD) via the DoD Physical Security Review Board (PSRB), DoD Security Enterprise Advisory Group, and Mission Assurance Coordination Board.

3. The ASN (RD&A) will:

a. Coordinate early in the research, development, and acquisition process concerning physical security requirements for DON material.

b. Provide Physical Security Equipment (PSE) acquisition and upgrade guidance to DON Services in support of DUSN conventional physical security, including Physical Access Control Systems (PACS), in accordance with reference (n).

c. Coordinate with the DON Chief Information Officer (DON CIO) to develop and maintain a technology solutions portfolio that identifies and specifies cybersecurity testing and accreditation requirements for DON Services in accordance with reference (o).

4. Director, Naval Criminal Investigative Service (DIR NCIS). DIR NCIS will:

a. Coordinate with DUSN regarding results of best practices and recommendations to inform physical security policy based on results of assessments and exercises as appropriate in accordance with reference (m).

b. Arm security, law enforcement, and counterintelligence personnel in accordance with reference (k).

5. The (ASN (EI&E)). ASN (EI&E) will:

a. Program physical security requirements in military construction projects through a formal process in accordance with reference (b).

b. Incorporate physical security standards as part of facility or building planning, construction, and acquisition in accordance with reference (b) and all appropriate DoD Unified Facilities Criteria (UFC).

c. Coordinate with the Deputy Under Secretary of the Navy Intelligence & Security (DUSN (I&S)) and DON Services for the planning of PSE funding and advocate for their needs at the SECNAV and OSD Cost Assessment and Program Evaluation levels.

d. Develop and manage Program Objective Memoranda in coordination with the Heads of the DON Services for the sustainment and lifecycle of PSE and interfaces.

6. The Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN (M&RA)). ASN (M&RA) will ensure the ability to verify status of individuals within the DON via Defense Enrollment Eligibility Reporting System for access to DoD installations and resources in accordance with references (c) and (l).

7. DON CIO. The DON CIO will coordinate with Defense Information Security Agency to integrate applicable cybersecurity controls into physical security standards consistent with references (b) and (r).

8. Chief of Naval Operations (CNO) and Commandant of the Marine Corps (CMC). The CNO and CMC will:

a. Coordinate with Combatant Commanders for requirements regarding this instruction and provide recommendations to the DUSN for policy and program change consideration.

b. Establish physical security measures to ensure the protection of DON assets to include appointing PSP Managers.

c. Establish and maintain responsibility for Service-specific requirements for PSP and measures.

d. Develop and implement policy, provide oversight, and evaluate the effectiveness of the Component's PSPs.

e. Program for and allocate sufficient budgetary resources to meet the minimum standards for physical security as established by Component PSPs and this instruction. Ensure investments are guided by a capital planning and investment strategy that is risk-managed and results based.

f. Provide information and assistance necessary to advance the DON PSP and by providing subject matter experts in support of Secretariat-level working groups.

g. Provide guidance for local commanders and civilian directors to determine recurring requirements and frequency for the vetting of non-Federal Government and non-DON-issued card holders based upon local security requirements using United States Government (USG) authoritative databases as prescribed within enclosure (4) of this instruction.

h. Implement and maintain a permissions and roles based (access hierarchy) system to allow for PSE requests and management of equipment inventory.

i. Prior to acquiring PSE, including but not limited to ESS (i.e., closed circuit television/surveillance systems), IDS, and Electronic Physical Access Control Systems (ePACS)), ensure conformance with minimum standards and guidelines, interoperability, and non-duplication of acquisitions. In addition, ensure the equipment supplier is on an approved General Services Administration (GSA) list of suppliers and not from a source which could be compromised by foreign or criminal elements.

(1) Ensure Information Technology (IT) systems comply with cybersecurity policy in accordance with reference (o) and are afforded adequate protection as pursuant to reference (p).

(2) Provide automated capabilities to verify and authenticate all DON-approved identity credentials used in DON PACS.

(3) Provide coordination for the implementation of biometrics within DON PACS in accordance with references (c) and (q).

(4) Support and facilitate the DON obtaining authorization to operate IT based PSE and ESS, under reference (r).

(5) Provide IT-support for physical security, to include:

(a) Interoperability of Common Access Card (CAC) attributes in computerized card and badging systems.

(b) Validity of CAC attributes against established DoD and DON information databases.

(c) Authenticity of CAC and CAC holder, using match-on-card and anti-counterfeit protection measures embedded in the CAC.

j. Direct local commanders and civilian directors to develop physical access requirements for local emergencies and first responders that require access during all-hazards events.

k. Conduct privacy impact assessments in accordance with reference (s) before implementing policy or programs that collect data from or about individuals who apply for physical access.

l. Ensure all subordinate commands comply with requirements and assignment of responsibilities as outlined in this instruction and service policy.

m. Establish procedures for physical security planning, construction, and acquisition of facilities or buildings in accordance with reference (b) and applicable DoD UFC.

n. Ensure the appropriate integration of the physical security and antiterrorism programs, to include the development and maintenance of an installation or facility-specific physical security plan consistent with references (g) through (i).

o. Coordinate response policies to physical security threats in accordance with references (g) through (i), (t), and this instruction.

p. Arm security, law enforcement, and counterintelligence personnel in accordance with references (k) and (u).

q. Provide specific guidance to commanders and civilian directors for installations, facilities, or portions thereof categorized as controlled or restricted. This guidance should detail additional security measures to be taken to safeguard the asset.

r. Develop a policy and maintain a process to request and record deviations from the minimum standards prescribed in

accordance with references (b), (c), (v), (w), and enclosure (5) of this instruction. The deviation policy will identify the process to request deviations to include periodic status reports and notification to the DUSN and DoD as required by reference (c) and this instruction.

s. Establish a physical access control program in accordance with references (c), (x), and enclosure (4) of this instruction.

t. Pursuant to reference (m), designate an individual to represent the Service in the DoD Physical Security Enterprise Analysis Group.

9. CNO. In addition to the responsibilities in paragraph 9 above, the CNO will designate Executive Agents for the DoD's Explosive Detection Equipment Research, Development, Test, and Evaluation program and the DoD's Key and Lock program in support of reference (n).

PHYSICAL SECURITY STANDARDS

1. Physical Access Control at DON Installation Perimeters and Facility Entrance Points. In accordance with reference (c), the grounds of DON installations and facilities on DON-owned or DON-leased land will have a perimeter barrier or boundary identification (such as a fence-line, wall, or signage), Access Control Point (ACP), and a method for processing visitors. The DON Services will establish access control and implement procedures for all populations to gain access pursuant to references (c), (w), (x), and enclosure (4) of this instruction.

2. Perimeter Control. Perimeter control measures will be constructed and deployed to:

a. Deter, detect, deny, delay, and defeat potential threats based on risk assessment.

b. Clearly identify controlled installations, facilities, and areas and communicate purposes for boundaries.

c. Channel pedestrian and vehicle traffic to intended areas and prevent accidental or unauthorized entry.

d. Optimize security force operations and enable them to maintain full control.

e. Optimize safe and efficient operation of the facility or installation.

f. Protect against reverse entry.

3. Intrusion Detection and Surveillance Systems

a. IDS

(1) IDS will be deployed to protect sensitive or critical areas and assets in accordance with applicable DoD, DON, and Service Policy.

(2) IDS implementation and operations will include planning, programming, and budgeting for life-cycle sustainment of systems to include training, testing, maintenance, and sustainment.

(3) All IDS signals will annunciate at a central control or monitoring location from which law enforcement or security forces can be dispatched.

(4) Central and local monitoring stations will be manned by certified operators.

(5) IDS procured by installation tenants must be coordinated with and compatible with the host installation's IDS. IDS that are incompatible with the host installation are not authorized.

(6) IDS must be configured to send an alarm to alert the alarm monitor of system tampering or line disruption.

(7) Testing of IDS must be conducted in accordance with the manufacturer's specifications and on a Service determined periodic schedule, or as dictated by higher order policy for the asset being protected to ensure operability and annunciation at the monitoring station.

(8) DON assets will be protected by IDS in accordance with applicable DoD, DON, and Service Policy. Assets protected by an IDS will report to a central monitoring station and/or will be checked during non-duty hours in accordance with references (a), (v), and (w).

(9) Records of monitoring or physical checks of areas protected by IDS systems will be maintained for a period of three years.

(10) Security Forces will respond to alarm annunciations in accordance with criteria established for the resource being protected by policy and/or agreement.

(11) Where DON assets or resources are stored off-installation in civilian communities, and where security checks cannot be conducted by DON personnel due to legal or operational considerations, liaison will be established with local law enforcement or security services to ensure non-duty hour checks are conducted by local authorities or in coordination with host nation authorities. DON entities in GSA leased facilities will

coordinate with GSA to have Federal Protective Services conduct security and antiterrorism/force protection support.

b. Surveillance Systems

(1) Surveillance Systems may be deployed to support protection of sensitive or critical areas and assets and to provide a deterrent, real time monitoring and/or archived video recordings for retrieval or evidence in accordance with applicable DoD, DON, and Service Policy.

(2) Surveillance Systems, implementation and operations should include planning, programming, and budgeting for technology refreshments and sustainment of systems to include testing and maintenance.

(3) Surveillance Systems should be configured to prevent tampering or line disruption and should have full diagnostic evaluations for operation and control of pan/tilt/zoom capabilities and archiving.

(4) Use of Surveillance Systems does not eliminate the requirement for security checks as directed by federal law, DoD, DON, and Service Policy.

4. Security Forces

a. Security Forces are an integral part of the PSP, and will be employed and operated in accordance with reference (y). Their roles and responsibilities in the establishment of an effective PSP are to:

(1) Provide deterrence through physical and visual presence.

(2) Neutralize or delay threats from reaching the protected resource until additional response forces arrive.

(3) Support IDS by providing armed security patrols for alarm activation when dispatched.

(4) Provide dedicated security response capability to protect resources critical to national defense.

(5) Support visual assessment needs for IDS alerts when electronic assessment capability is unavailable or inoperative. Under these circumstances, Security Forces can provide the capability to classify and characterize threats as hostile or non-hostile, identify the threat, and determine if additional response forces or specialized response forces are required to neutralize a threat.

(6) Provide detection and warning capability when IDS sensors are inoperative or IDS is unavailable by posting personnel at the protected resource or asset in accordance with DoD, SECNAV, and Service Policy.

(7) Conduct access and circulation control activities for military installations, and for locations with restricted and/or controlled areas in accordance with DoD, SECNAV, and Service Policy.

b. When conducting security planning, considerations must include:

(1) Security force requirements as directed in DoD, DON, and Service Policy including Status of Forces Agreements/Host Nation Agreements where appropriate.

(2) Legal aspects for use of force (to include deadly force).

(3) Requirements for communications equipment (e.g., radios, landlines, computers, control centers, IDS, etc.) to support security force operations to include whether communications equipment must provide secure or non-secure means of communications. Further consideration will be given to provide a capability to communicate with local law enforcement and first responders.

(4) Weapons to be employed by armed security forces, to include lethal and non-lethal capabilities such as Military Working Dogs (MWD), riot control agents, etc.

(5) Vehicles used by response forces (to include armored or unarmored vehicles and harbor security boats).

(6) Personal Protective Equipment to be used by security force members, to include ballistic armor, helmets, gas masks, etc.

(7) Availability of host nation or local law enforcement and/or security services support to the installation. Where assets or resources are stored in DON installations or off-installation in civilian communities, and where security checks cannot be conducted by DON personnel due to legal or operational considerations, liaison will be established when possible with local law enforcement or security services to ensure that non-duty hour checks are conducted by local authorities or in coordination with host nation authorities.

5. Security Lighting

a. Security lighting equipment and placement will be sufficient to provide visibility for the detection, assessment, and interdiction of unauthorized activity at DON installations, facilities, entries, checkpoints, controlled areas, and restricted areas.

b. The effect of security lighting on vulnerabilities and potential threats must be considered and authorized personnel must have the means to direct or disable lights for defense against potential threats.

c. Security lighting systems, switches, power lines, and supporting equipment will be designed and fielded to ensure intruders and unauthorized personnel cannot easily defeat the systems.

d. Periodic inspections of security lighting equipment must be conducted, at a minimum of monthly, to identify deficiencies and ensure continued operability.

e. Alternate power sources, stand-by power sources, battery-sustained emergency lighting, hand-held lights, or portable lights will be deployed as needed to meet security lighting objectives for a given installation, facility, entry point, check point, controlled area, or restricted area.

6. Asset and Resource Protection

a. Physical security policies and measures will provide for the physical security of DON assets that require special security measures to protect them from theft, damage, unauthorized access, and unauthorized disclosure. Specific security policies and measures are directly correlated to the resources being protected in accordance with references (a) and (w).

b. Physical security plans for protection of DON assets will address responsibility for the security of assigned or transient assets and resources while temporarily located at a facility or installation.

7. Key, Combination, and Lock Control

a. DON Commanding Officers of installations, tenant commands, and agencies will implement procedures to ensure accountability and control of access cards and credentials, combinations, keys, and locks for controlled and restricted areas and protected assets.

b. DON Commanding Officers of installations, tenant commands, and agencies will appoint Access Control Custodians in writing who will maintain key and combination control registers to achieve continuous accountability.

c. Keys and combinations will only be accessible to those individuals whose official duties require access. A current roster of personnel who are authorized access will be maintained and kept from public view.

d. The number of keys and combinations issued will be held to the absolute minimum.

e. Inventories of keys, combinations, and locks will be conducted periodically except for AA&E which will be inventoried semi-annually by a disinterested third party or person not responsible or authorized unaccompanied access. Inventory records will be retained in activity files in accordance with DON Component guidance.

f. If keys or combinations that protect installations and assets are lost or stolen, the affected locks or lock cores will be replaced immediately. The compromise of keys or combinations to installation perimeters and AA&E will be immediately reported to the installation commander, director, or designated representative.

g. Combinations will be changed when locks are placed into use and whenever persons knowing the combination no longer require access (unless other sufficient conditions exist to prevent that individual's access to the lock) or when combinations have been subject to compromise.

h. Unserviceable high-security padlocks, keys, and cylinders will be controlled until destroyed in accordance with DON Component policy or direction provided by the DoD Lock Program.

i. Sensitive conventional AA&E key and lock controls will be implemented in accordance with references (z) and (aa).

j. Combinations used to protect classified information and resources will require the custodian to hold a personnel security clearance commensurate with the highest level of classified information being protected, in accordance with reference (p).

8. Unmanned Systems (UXS) to include but not limited to Unmanned Aerial System (UAS) and Unmanned Underwater Vehicles (UUV)

a. UXS, UAS, and UUV intrusions onto installations and DON Areas of Responsibilities continue to increase in number. The DON Service Policy will require response, reporting, and processing if collected on DON property or assets.

b. Coordination will be established in operating standards for installation, federal, and local cooperation to deter, prevent, and respond to intrusions and seizures.

c. All incidents will be reported via the Operational Reports system with the DUSN (I&S) and NCIS in the info line.

9. Physical Security Surveys

a. A physical security survey is a formal recorded assessment of an installation or facility's overall PSP to include electronic security. The survey provides the commander or director with an assessment of the security posture in view of the threat and mission, and informs the commander or civilian director of the installation's physical security strengths and weaknesses.

b. Formal, recorded surveys will be conducted by qualified personnel in accordance with service guidance.

c. Survey reports will record findings of policy deficiencies and observations concerning potential means to improve site security. Until the DoD issues a DD Form to record the results of these surveys, the DON Services will develop their own means of gathering and recording survey and inspection information. Procedures and measures to evaluate will include:

(1) Threat assessment procedures.

(2) Security Forces description, availability, training, equipment, and guard/post orders.

(3) Implementation of access control procedures pursuant to enclosure (4) of this instruction.

(4) Control of visitors and packages.

(5) Use of PSE.

(6) Security lighting.

(7) Control, issuance, and accountability of keys and access credentials used at the installation perimeter, enclaves, and facilities such as for limited access gates and for industrial spaces.

(8) Identification of critical areas or facilities.

(9) Process used to track work orders addressing discrepancies.

(10) Current, submitted, or expired waivers and exceptions to policy.

d. Surveys will be conducted as prescribed by Service Component except:

(1) When no record exists of a previous physical security survey for a facility requiring a survey and for pre-occupancy of that facility.

(2) When the commander or director determines a greater frequency is required.

(3) AA&E surveys will be conducted at intervals not to exceed 12 months.

e. Physical security surveys will include:

(1) An executive summary for the commander or director.

(2) A detailed assessment of the security posture of the installation or facility.

(3) Recommended prioritization of resources for reducing vulnerabilities.

(4) Exhibits, such as photographs, sketches, graphs, and charts to clarify findings and recommendations, and assessments of criticality and vulnerability.

f. A copy of the physical security survey, and exhibits (if beneficial) will be provided to:

(1) The commander or director of the installation or facility.

(2) The installation Antiterrorism Officer.

(3) The Regional Security Director.

g. The survey will be used to develop a corrective action plan to address upgrades, repairs, modifications to procedures, and will include fiscal resources required to support

prioritization. Highest priority should be given to activities considered essential to mission accomplishment. Forward this plan to the commander or director for approval and inclusion in the physical security plan.

h. All survey reports will be signed and completed by the inspector completing the inspection within 30 days of the scheduled survey date.

i. Surveys will be maintained on file for three years.

10. Controlled and Restricted Areas

a. A controlled area is an area in which access to the general public is denied, unless certain entry control measures are met. Commanders and directors will establish operational policy for controlled areas. This type of area has the least restrictive conditions. The requirements for entry include a military ID card or proof of ID by another federal or state government document, and a need for access. Once authorized to enter, movement within the area is not controlled. All DON installations, Operational Support Centers/Reserve Centers, and buildings not accessible by the general public because entry is controlled by proof of ID that the individual is an active, retired, or authorized veteran of the military (i.e. commissary, exchange, clinic) will be designated as controlled areas and granted entry via a controlled access point and the access control requirements of reference (c).

b. Restricted areas. A restricted area is an area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas are always inside of controlled areas. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation commander, activity commander, or director, posted in accordance with reference (b), and will employ physical security measures. Tenant commanders designating restricted areas within the confines of their compounds will coordinate with the host commander to ensure their designated restricted areas are on the installation’s restricted area list and that the protection

required for the asset can be provided by the host and unit security personnel.

(1) Restricted areas must be established in writing by the Commanding Officer within his or her jurisdiction in accordance with reference (b). Designated restricted areas will be a part of installation physical security plans.

(2) Tenant commanders and directors will publish and inform the host commander, in writing, of all areas under their control that are designated as restricted areas. Particular attention will be paid to those areas that are vital to national security, to include task critical assets.

(3) Installation commanders and directors will publish a consolidated list of all restricted areas aboard the installation, including tenant command restricted areas. This list will be contained in the unit and installation Anti-terrorism Plan in which the Physical Security Plan may be included, will be reviewed annually, and will specify which areas are vital to National Security.

(4) DON Services will ensure restricted areas are established around assets and facilities to protect mission-critical or sensitive assets or programs, security interests, classified material, nuclear material, conventional AA&E, Research, Development, Test, and Evaluation AA&E facilities, drugs, precious metals or precious metal-bearing articles, articles or funds having high likelihood of theft, and certain unclassified chemicals.

(5) When the decision is made to designate an area as restricted, the Commanding Officer will further identify entry requirements, including:

(a) Personnel authorized access.

(b) Visitor control.

(c) Identification systems.

(d) Access control procedures.

(e) Security clearance requirements (including any requirement for maintenance and custodial personnel).

(6) In designating restricted areas, Commanding Officers must identify the level of restricted area to be established as described below. All restricted areas will be posted simply as restricted areas so as not to single out or draw attention to the importance or criticality of an asset. Lower level restricted areas will not be located inside of higher level restricted areas i.e. a Level One restricted area will not be located inside of a Level Two restricted area.

(a) Level One

1. The least secure type of restricted area. It will be established to provide an increased level of security over that afforded elsewhere aboard the activity to protect a security interest that, if lost, stolen, compromised, or sabotaged, would cause damage to the command mission or impact upon the tactical capability of the United States. It may also serve as a buffer zone for Level Two and Level Three restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement within it may or may not permit access to a security interest or asset.

2. At a minimum, Level One restricted areas will be established around category III and IV AA&E storage facilities; defense infrastructure; petroleum, oil, and lubricants, power, and water supply and storage areas; pier facilities for amphibious, auxiliary, and Military Sealift Command ships; Strategic Sealift Ships; prepositioned ships, mine warfare and coastal patrol ships; controlled drugs and precious metals; funds and negotiable instrument storage areas; security force facilities; emergency dispatch centers; electronic security system monitoring spaces and Military MWD facilities; motor pools; and research, development, test, and evaluation centers; or other sites whose loss, theft, destruction, or misuse could compromise the defense infrastructure of the United States.

(b) Level Two

1. A Level Two restricted area may be inside a Level One area but will not be inside a Level Three area. It will be established to provide the degree of security necessary to protect against uncontrolled entry into, or unescorted movement within, an area that could permit access to a security interest that, if lost, stolen, compromised, or sabotaged, would cause damage to the command mission or harm the operational capability of the United States. Uncontrolled or unescorted movement could permit access to the security interest.

2. At a minimum, Level Two restricted areas will be established around defense early warning alert systems, forces, and facilities; pier facilities for carriers, submarines, and large deck amphibious ships; aircraft hangars, ramps, parking aprons, flight lines, runways, and aircraft rework areas; all risk category arms and category I and II AA&E storage facilities and processing areas (including ammunition supply points); essential command and control, communications, and computer facilities, systems, and antenna sites; critical assets power stations, transformers, master valve, and switch spaces; and assets whose loss, theft, destruction, or misuse could impact the operational or tactical capability of the United States.

(c) Level Three

1. The most secure type of restricted area, it may be within less secure types of restricted areas and will be established to provide a degree of security where access into the restricted area constitutes, or is considered to constitute, actual access to a security interest that, if lost, stolen, compromised or sabotaged, would cause grave harm to the command mission or strategic capability of the United States. Access to the Level Three restricted area will constitute actual access to the security interest or asset.

2. At a minimum, Level Three restricted areas will be established around Presidential Support Mission Facilities; nuclear, special/nuclear weapons research, testing, storage, and maintenance facilities; critical command and control, communications, and computer facilities, systems, and antenna sites; critical intelligence-gathering facilities and systems; nuclear reactors and category I and II special nuclear materials; permanent or temporary pier facilities for fleet

Ballistic Missile Submarines armed with nuclear weapons; and assets whose loss, theft, destruction, or misuse would result in grave harm to the strategic capability of the United States. Facilities identified by the Geographic Combatant Commander (GCC) as having strategic significance will be designated and protected as a Level Three restricted area.

(7) Decisions regarding designations of restricted areas, their levels, and criteria for access to each restricted area are at the discretion of the commander or director, except in cases:

(a) Where higher headquarters guidance has been provided for the protection of specific assets (e.g., classified material, sensitive compartmented information, automated data processing systems, nuclear weapons, conventional AA&E, and nuclear reactors and special nuclear material).

(b) Where direction has been provided by higher headquarters, commanders, and directors will ensure the minimum security measures are employed for restricted areas to include a clearly defined protected perimeter, controlled access limited to those with appropriate clearance and "need-to-know", establishment of a personnel identification system, maintenance of access list and visit log documentation, performance of checks for unauthorized entry, and designation of a response force.

(8) Service Policy will require that activities with restricted areas establish a system to check restricted areas, facilities, containers, perimeter, or building entry and departure points by occupants/users in an attempt to detect any deficiencies or violations of security standards.

11. Signs and Posting of Boundaries. Signs will be posted as part of establishing the legal boundaries of an installation and around restricted areas with applicable DoD and Unified Criteria Facilities guidance.

12. Barriers and Openings

a. Sufficient barriers will be in place to control, deter, delay, and deny access by unauthorized persons.

b. Inspections will be performed periodically to ensure barriers continue to function as needed. Barriers will be sustained and placed on a phased replacement plan as necessary to ensure continued operation and protection of assets.

INSTALLATION ACCESS CONTROL

1. General

a. Pursuant to reference (c), the DON Services will field ePACS at all installations. Fielded ePACS must interface with the Identity Matching Engine for Security Analysis (IMESA). The Services will fund the operation, maintenance, and enhancement of IMESA with additional government data sources as those sources become available. Where an ePACS are not in use, the minimum standard for controlling access is by physical and visual inspection of credentials as outlined in reference (c).

b. Access control standards will include identity proofing and vetting to determine the fitness of an individual for access to DON installations and facilities.

(1) The DON will utilize the SECNAV Form 5512/1 as the sole means to collect Personally Identifiable Information (PII) for the purpose of installation access control. Collected PII will be used to conduct background checks on non-DoD affiliated visitors, contractors, and vendors. Each time a background check is conducted, personnel requesting access will complete the SECNAV Form 5512/1 for accountability purposes. Use of any locally produced or other forms to collect and/or maintain PII is strictly prohibited.

(2) Installations will maintain the original copy or an electronic copy of all completed SECNAV 5512/1 forms for a minimum of three years to support periodic audits.

c. Only trained military and government civilian personnel delegated by commanders or civilian directors will perform access control duties that include identity proofing, vetting and determination of fitness, access authorizations and privileges, and issuance of appropriate and authorized cards or passes.

(1) The DON Services will establish a training program to ensure personnel conducting access control duties understand and are capable of performing tasked functions.

(2) Vetting must be conducted by a certified and trained National Crime Information Center (NCIC) terminal operator.

(3) Determination of fitness must be conducted by a government employee (military or civilian).

d. Identification documents authorized for use in issuance of credentials or a visitor pass are limited to those listed in reference (c) and paragraph 3 of this enclosure.

e. Pursuant to reference (c), all persons granted unescorted access to DON installations and facilities must possess an authorized and valid credential. Such credentials will be issued only after:

(1) A determination of a valid purpose to enter.

(2) The completion of identity proofing and vetting.

(3) A favorable determination of fitness.

f. The CAC (simultaneously establishes identity, historic fitness, and purpose) and the Local/Regional Credential (LRC), as controlled items, will not be utilized in temporary badge issuance exchanges as defined in reference (b).

g. LRCs will not be issued for individuals in possession of an alternate approved credential (e.g., CAC, DoD ID, Real ID, etc.). Required LRC characteristics are described in paragraph (7) of this enclosure.

h. Enrollment conducted at DON installations will be reciprocal within the DON and will be accepted as proof of historic fitness. Individuals who have been previously vetted and issued a LRC at a DON installation connected to IMESA through the ePACS will be automatically registered at another IMESA equipped installation by presenting the same credential for access at the visitor control center as long as proof of a valid purpose for access is provided.

i. Purpose for accessing an installation varies depending on several factors to include installation type, mission, services offered, and current Force Protection Condition (FPCON), credential presented, special events, etc. As purpose is so variable, approval of purpose for entry is at the discretion of the installation commander or director.

j. The DON Services may authorize the establishment of trusted traveler programs at ePACS-enabled installations in accordance with reference (c).

(1) Individuals bringing co-travelers aboard DON installations in this manner will be personally accountable for the conduct of their guests while aboard the installation.

(2) Service or installation policy will determine the number of co-travelers an individual may vouch for at any one time.

(3) Non-United States citizens are not permitted to sponsor co-travelers under these programs, to include foreign nationals in possession of a blue stripe CAC or DoD dependent ID card.

k. Per reference (c), the DON Services may implement unmanned Access Control Points (ACPs). These ACPs will meet the requirements of reference (c) and will include two-factor authentication. Unmanned ACPs capable of allowing vehicular access require consideration from the Under Secretary of Defense for Intelligence & Security (USD (I&S)) before being operated in the unmanned mode. Packages requesting this consideration will be forwarded to the DUSN (I&S). Such requests require endorsement at the 3-Star level at a minimum from the Operational Commander and CNO/CMC levels. Per reference (c), ACPs with at least one on-site attendant servicing multiple lanes are not considered unmanned.

l. The DON Services may authorize more restrictive access control requirements than those required in reference (c) based upon the type of installation, security level, and category of individuals requiring access, FPCON, and level of access to be granted, however, per reference (c), this requires an approved deviation. Deviations required due to the application of these more restrictive access control requirements will be approved by the UNSECNAV via the SDI&S. Deviation requests will be forwarded to the DUSN (I&S). Such requests require endorsement at a minimum of 3-Star level at the Operational Commander and CNO/CMC levels.

m. Where circumstances prevent the use of the CAC, Personal Identity Verification (PIV), or Personal Identity Verification - Interoperable (PIV-I) because of specific circulation control requirements (such as the requirement to have a visible distinction for clearances, authorizations, or security functions), the issuance of a supplemental badge is authorized. These credentials will not be used in place of approved access credentials at perimeter ACPs. The LRC will not be used in place of approved access credentials at enclave or facility entry control points. Supplemental credentials will be limited to visually verify access to a restricted area.

n. Accountability of DON Sponsored Foreign Personnel. The DON Services will use the Foreign Visits System - Confirmation Module to document the occurrence of DON sponsored official visits by foreign nationals to DON Services consistent with references (c) and (ac), and will incorporate this requirement in their relevant directives.

o. PACS Failure Contingency Plan. During contingency operations (e.g., in the event ePACS is not operational), other methods may be employed. All local passes issued without a barcode that cannot be read electronically, should be laminated after a unique authenticator is placed on the credential (e.g., local stamp overlapping the picture and pass prior to lamination, Infrared stamp, number authenticator, etc.) and will be carried by the visitor at all times while on the installation. Once the contingency operation is over and/or PACS becomes operational, visitors that have been issued a local pass or credential will be directed to the issuance facility to receive an LRC or pass. Possession of the pass will signify that all processing actions (sponsorship/purpose, identity proofing, vetting, and fitness determination) have been completed by the issuing authority.

2. Service/local level access control policy will:

a. Establish procedures for physical access control applicable to all installation perimeters and ACPs to include airfields and water ports that permit access to a military installation by an individual.

b. Mandate the use of deployed DON ePACS to the maximum extent possible. Monitor use of and report to DUSN (I&S)

anomalies unable to be resolved by the Service. Per reference (c), all credentials will be scanned at all times with exception of United States citizen CACs which may be randomly scanned during peak traffic periods or special events. All foreign national IDs to include (blue stripe) CACs and United States IDs will be scanned at all times.

c. Require a training program for perimeter security personnel, including at both the ACP and Visitor Control Center (VCC), on the requirements, processes, and prohibitions described in reference (c) and this enclosure.

d. Establish a redress and appeal process for disqualifying conditions in this section, including each criminal conviction(s), in determining the fitness of non-DoD persons seeking access to DON installations. Installation commanders and directors must still evaluate non-DoD persons against the DON established fitness standards.

e. Require that credential requirements, fitness disqualification standards, redress and appeal processes, and a Privacy Act statement are clearly and conspicuously posted at all VCCs and on existing or new installation websites.

f. Include a determination, or list of, acceptable purposes for accessing installations in accordance with reference (c), this enclosure, applicable federal, state, and local laws, and other applicable DoD and SECNAV policy.

g. Require coordination with local first responders to establish appropriate standard operating procedures for facilitating access to first responders during emergencies.

h. Require an alternate means to process visitors through the visitor control process when the VCC is closed.

i. Establish a process for processing persons identified with an active warrant for both the Continental United States (CONUS) and Outside CONUS (OCONUS) installations.

j. Address trusted traveler programs in accordance with the requirements of reference (c) and paragraph 1.j of this enclosure.

k. Identify and specifically address limitations and unique requirements for vetting and fitness determinations for installation and facility access (OCONUS).

l. Address all possible categories of persons to include but not limited to:

(1) Military personnel (retired, active, and reserve) and personnel acting on their behalf.

(2) DON civilians (active and retired).

(3) DON contractors.

(4) Persons in possession of federal PIV credentials.

(5) Persons with DON-approved non-federally issued PIV-I credentials.

(6) Foreign visitors.

(7) Tenants and tenant command responsibilities.

(8) Vendors (e.g., food delivery, parcel delivery, personnel transportation companies).

(9) Non-affiliated personnel living in Public-Private Venture housing on a DON installation or property.

(10) Local first responders and law enforcement personnel.

(11) Red Cross and United Services Organization employees, contractors, and volunteers.

(12) Drivers for transportation network companies (i.e. Uber, Lyft).

m. Require random inspections of persons, packages, and vehicles at ACPs per reference (a). These inspections will comply with legal and jurisdictional requirements.

n. Address special events and circumstances.

(1) Requirements for physical access for special events, circumstances, or activities of limited duration will be addressed and will include compensatory measures when the requirements of reference (c) and this instruction cannot be met.

(2) For facilities that are open to the public or located outside of the installation perimeter (e.g., golf courses, museums, and off-installation housing), local policies and procedures will address physical access when the FPCON is elevated.

3. Establishing Identity for Unescorted Access

a. Per reference (c), persons granted unescorted access must be identity proofed. Identity is established by providing a valid and original form of identification or combination of source identity documents listed in reference (c), or paragraphs 3.d, 3.e, and 3.f of this enclosure.

b. Documents provided will be screened for evidence of tampering, counterfeiting, or other alteration and documents that appear questionable (e.g., having damaged laminates) or otherwise altered will not be accepted.

c. Altered documents will be held until appropriate authorities are notified, and disposition procedures are authorized.

d. Identity documents in reference (c) and listed below will be accepted for the establishment of the individuals identity. All documents must be current.

(1) Permanent resident card or Alien Registration Receipt Card (INS Form I-551).

(2) Employment authorization document (INS Form I-766).

(3) United States Coast Guard Merchant Mariner Cards/Credentials.

(4) Department of Homeland Security (DHS) "Trusted Traveler Cards" (Global Entry, NEXUS, SENTRI, FAST).

(5) Border Crossing Card (Form DSP-150).

(6) Native American Tribal Photo Identification.

(7) Veteran's Health Identification Card (VHIC). The VHIC is used primarily for the purpose of identification and processing for Department of Veterans Affairs (VA) medical benefits and does not by itself facilitate access to DON installations. The VHIC will establish identity and provide purpose for the holder to access DON installations where eligible benefits (medical, commissary, exchange, and Moral Welfare and Recreation (MWR) facilities) exist. Eligible veterans solely under the Purple Heart and Disabled Veterans Equal Access Act of 2018 (veterans who are Purple Heart recipients, former Prisoners of War (POW) and VA-documented service connected disability rating of 0-90 percent) can present their VHIC to gain entry to DON installations for the purpose of commissary, exchange and MWR facilities.

(a) Eligible veterans will provide their VHIC at installation visitor centers to validate eligibility. The VHIC must display the veteran's eligibility status (i.e., Purple Heart, Former POW, Service Connected, or VA Healthcare Enrollee).

(b) The veteran must be vetted, fitness determined, and entered into the ePACS. Veterans with felony convictions, felony arrest warrants, or other types of derogatory information related to criminal history or terrorism will not be permitted entry.

(8) Veteran Family Primary Caregivers ID. The VA will develop a new ID for primary family caregivers of an eligible veteran under the Program of Comprehensive Assistance for Family Caregivers at a future date. Until that new ID is developed, VA will issue a letter from the VA Office of Community Care that indicates the individual is approved and designated as the primary family caregiver. This letter establishes purpose for installation access for the use of commissaries, exchanges, and MWR retail facilities. The caregiver must be identity proofed and vetted in accordance with reference (c) and this enclosure prior to allowing unescorted access to DON installations.

e. In addition to identity proofing documents listed in paragraph 3.d above, parents or legal guardians may provide any of the following credentials for the purpose of identity proofing for persons under the age of 18 who do not possess a photo ID.

(1) School record, school identification, or report card.

(2) Day care or nursery school record.

(3) Original or certified copy of birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal.

f. The Services may utilize the below additional supplemental sources of identity proofing in concert with documents listed in paragraph 3.b above to further substantiate identity.

(1) United States Military or draft record.

(2) Native American Tribal Document provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address.

(3) United States Social Security card issued by Social Security Administration.

(4) Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350).

(5) United States Citizen ID Card (Form I-197).

(6) Foreign Military or Host Nation Government Identification Credentials.

g. Identity proofing OCONUS will be determined by the GCC in accordance with Status of Forces Agreement or international agreements. For OCONUS locations, commanders will coordinate with local and foreign authorities to identity proof applicants to the greatest extent practical and lawful.

4. Establishing Fitness for Unescorted Access

a. Pursuant to reference (c), an individual's fitness will be established before granting unescorted access to DON installations or facilities. Fitness for access has two elements: historic fitness and current fitness.

b. Once an individual has undergone successful identity proofing, installation commanders and directors must determine the individual's fitness for installation access, that is, the local determination of whether an individual poses an unreasonable threat to DON resources or personnel if granted installation access.

c. Historic fitness determination. At a minimum, installations will determine historic fitness of individuals through NCIC Interstate Identification Index (NCIC-III), relevant government databases (to include the Terrorist Screening Database (TSDB) when available), and the Service criminal justice information system.

d. In addition to the on-the-spot review and adjudication conducted by government personnel, proof of historic fitness may also be determined by:

(1) The acceptable credential used to establish identity, if listed as establishing historic fitness in section 5 of reference (c).

(2) A previously conducted review and adjudication at an installation if followed, immediately and without lapse, by enrollment in the IMESA for continuous vetting (i.e. issuance of a Defense Biometric Identification System (DBIDS) credential).

(3) The DoD Consolidated Adjudication Facility (CAF), or predecessor organization, determination that the individual eligible for access to classified information, so long as that eligibility remains in scope.

(4) A favorably adjudicated Tier 1 or higher background check performed by the DoD CAF or other Federal Agency that remains in scope.

e. Current fitness is established, on a recurring and continuing basis, through a review (either on-the-spot at the VCC or nightly through IMESA) of an individual's current derogatory information through a check of authoritative government sources which include:

(1) Terrorism lists, such as the NCIC Known and Appropriately Suspected Terrorist file and the TSDB.

(2) Felony wants and warrants, such as those listed in the NCIC Wanted Persons File.

(3) Barment order lists, such as relevant Service criminal justice information systems.

(4) Other relevant government databases that may be available such as:

(a) Other NCIC files (including the National Sex Offender Registry).

(b) Criminal justice or immigration databases.

(c) DoD's Automated Biometrics Identification System (ABIS).

(d) The Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System.

(e) DHS E-Verify and U.S. VISIT.

(f) Department of State Consular Checks (non-United States citizen).

(g) Additional data sources queried that are not listed must be approved by the servicing legal office.

(5) For OCONUS locations, commanders will coordinate with local and foreign authorities to vet applicants to the greatest extent practical and lawful.

(6) At OCONUS locations, installations may deviate from the requirements where local conditions, treaties, agreements,

and other foreign governments and allied forces require different standards.

5. Escorted Access. Personnel who require access without determination of fitness must be accompanied by a sponsor with authorization to escort individuals. The escort requirement is mandated for the duration of the visitation period. Escorted personnel must remain with their escort at all times. The Services will develop formal training for installation access sponsors and/or escorts. Pursuant to reference (c), all escorts must be United States citizens.

6. Fitness Adjudication Standards

a. Reference (c) requires that individuals establish their fitness, composed of distinct historic fitness and current fitness determinations, before being granted unescorted access to a DoD installation. Reference (c) and this enclosure establish the specific checks that must be performed to establish historic fitness and current fitness for unescorted access to DON installations and facilities. This paragraph establishes the DON standard to be used in making those determinations.

b. Standards for historic fitness. Historic fitness is established, at a specific point in time, only by means of a review of an individual's criminal history record information through a check of the NCIC III, and other relevant government databases and Service criminal justice information systems. The results of those checks are evaluated for:

(1) Criminal convictions. It is a disqualifying condition if an individual has been convicted:

(a) At any point of the felonies, or the attempt to commit or conspiracy to commit any of the felonies, as identified by uniform offense code, listed in Table 1.

(b) Within the last 10 years of any other felony.

(c) Within the past three years of any two misdemeanors.

(2) Failure to return credentials. It is a disqualifying condition if a non-DoD person has failed to return a previously-issued LRC upon termination or separation prior to the expiration of the LRC. This condition can be resolved one time with a written letter explaining why they failed to return the previously-issued LRC and confirming their understanding that failure to return a second LRC will disqualify them from receiving future unescorted access. LRCs that are not returned upon expiration are not considered "failure to return."

(3) Installation commanders and directors may disqualify any non-DoD person on a case-by-case basis for other articulable factors, based on a determination that the individual potentially poses an identifiable threat to order, discipline, health, or safety of the people or materiel on the installation, so long as those disqualifications are not arbitrary or discriminatory and are not based on specific criminal criteria other than those listed in paragraph 6.b. above.

Offense Categories
Treason
Espionage
Sabotage
Sedition
Military desertion
Homicide other than negligent vehicular manslaughter
Sexual assault or rape
Armed robbery
Arson
Aggravated assault with a gun or weapon, or on a law enforcement officer
Child molestation
Sexual exploitation
Firearms or explosives other than threats

Table 1. Lifetime Disqualifying Criminal Convictions

c. Standards for current fitness. Current fitness is established, on recurring and continuous basis, only by means of

a review of an individual's current derogatory information through a check of authoritative government sources for:

(1) Criminal justice related disqualifying offences. It is a disqualifying condition if an individual is:

(a) Listed in the NCIC:

1. National Sex Offender Registry.

2. Known or Appropriately Suspected Terrorist File.

3. Foreign Fugitive File.

4. Wanted Persons File.

5. Violent Person File.

(b) Currently subject to a felony want or warrant, regardless of offense.

(c) Currently on trial for any felony offense.

(2) Terrorism-related disqualifying conditions. It is a disqualifying condition if an individual is a confirmed match for an entry in the TSDB. All potential TSDB matches must be confirmed in accordance with reference (ad) prior to becoming a disqualifying condition.

(3) Barment. It may be a disqualifying condition if an individual is currently barred from another DoD or federal installation or facility. The installation commander must review the circumstances of each such instance to determine whether the individual should be disqualified.

(4) A claimed identity that cannot be verified based on the reasonable belief that the person submitted fraudulent identity information in the attempt to gain access.

d. Optional criteria. Depending on the specific characteristics of an installation, it may be a disqualifying criteria for an individual to not be a United States citizen or to not hold an active security clearance of a particular level.

e. Unless a non-DoD individual has a disqualifying condition under this section, they are determined fit for unescorted access to the grounds of a DON installation.

7. LRC Characteristics. LRCs issued by DON installations will be designed to meet the following characteristics:

a. Must comply with the "ID-1" definition in the International Organization for Standardization (ISO) 7810 standard.

b. If intended for use as a contact smartcard, must comply with the ISO 7816 standard.

c. If intended for use as a contactless smartcard, must comply with the ISO 14443 standard.

d. Must be visually distinguishable from the Federal PIV and the DoD CAC.

e. Must include:

(1) The individual's full legal name, printed in black text.

(2) The date of issuance.

(3) The date of expiration, not to exceed one year from date of issuance.

(4) A facial photo.

(a) Religious headwear is permitted if it does not obscure the face and is worn regularly by the individual.

(b) Vision correction glasses are permitted if they do not obscure the face and are worn regularly by the individual.

(c) Sunglasses are prohibited.

(5) The name of the issuing DoD Component and the name of the issuing installation or facility.

(6) A credential serial number or identifier, unique within the Component.

(7) Language identifying that the credential:

(a) Is property of the DoD.

(b) Does not convey any association with or eligibility for benefit from the DoD.

(c) Is not valid for any purpose other than for access to DoD installations or facilities.

(8) A no-reciprocity indicator, if issued in accordance with reference (c).

(9) A mechanism to electronically authenticate the credential using one of the methods described in low or medium risk in reference (c).

f. May include:

(1) A barcode.

(2) The individual's Local Population Electronic Data Interchange Personal Identifier.

(3) An escort authority indicator.

(4) An armed indicator.

(5) Time of day and day of week indicators.

(6) A FPCON indicator.

(7) Language providing a return mailing address and guaranteeing return postage.

(8) Language describing the prohibitions contained in reference (ae).

(9) The text "USA" indicating United States citizenship if the individual has proven that they are a United States

citizen. United States citizenship may be proven by any of the below:

(a) Valid United States passport or passport card

(b) Original or certified copy of a birth certificate issued by a state, United States territory, or the District of Columbia.

(c) Consular Report of Birth Abroad issued by the Department of State.

(d) Certificate of Naturalization issued by the United States Citizenship and Immigration Services (USCIS)

(e) Certificate of Citizenship issued by DHS or USCIS.

(10) Other visual security features.

g. May not include the individual's Social Security number in any manner.

8. Foreign Nationals. Foreign national visits may be for official or unofficial reasons. Official foreign national visits are normally handled through the Foreign Visits System. Unofficial foreign national visits are at the discretion of the installation Commanding Officer and must be approved in advance.

a. Certain Foreign Nationals and their dependents may be issued "blue stripe" CACs, DD-2765s, DD-1173s, "blue stripe" Next Generation Uniformed Services ID Card. Foreign nationals in possession of these access credentials are required to be explicitly registered into PACS at each installation they are assigned or otherwise have official duty.

b. Foreign students/visitors on official business will carry approved Invitational Travel Orders (ITOs) or Visit Requests on their person while on the installation and will present them to installation security forces when requested for the purpose of determining the need for access.

(1) In order to facilitate first-time entry, security forces should receive notification and must receive a copy of

ITOs or Visit Requests from the sponsoring unit prior to arrival of foreign nationals and/or their dependents. The United States military or civilian sponsors must be present during the initial processing of all foreign nationals for access. Once the foreign national has been positively identified and their need for access validated, they will be issued a visitor pass to allow initial access to the installation until they receive a more appropriate access credential (e.g., CAC, "blue stripe" Next Generation Uniformed Services ID Card, DD Form 1173, etc.) if applicable.

(2) Once a foreign national has been issued an access credential, it will be explicitly registered in ePACS for the installation which they are assigned or have official duty. Installations must validate foreign nationals' access credentials via ePACS to confirm the foreign national's access authority. All access credentials issued to a foreign national will be scanned prior to authorizing access to DON installations and/or facilities and will not be verified visually under any circumstance. Holders of foreign national credentials cannot serve as escorts onto any installation or vouch for co-travelers through the trusted traveler program under any circumstance.

(3) Official travel to any other military installation must be approved by the foreign national's sponsoring unit via official orders. Unofficial (leisure) travel to any other installations is not authorized. Note: Restrictions and authorizations for official or unofficial travel will be identified on official orders.

(4) If a foreign national is reported absent without leave (AWOL) or unauthorized absence, the sponsoring unit will coordinate with security forces to immediately flag that student and their dependents in ePACS. Foreign nationals that are reported AWOL or unauthorized absence must also be reported to the DON Insider Threat Analytic Hub at insiderthreat.fct@navy.mil.

c. Foreign military attachés. Foreign military attachés and their staffs are accredited diplomats vetted and cleared through the United States State Department and assigned to their diplomatic mission located in the National Capital Region (NCR). They do not receive orders from the DoD, but are officially based in the United States as diplomats. Foreign military

attachés often have valid official business at DON installations which will fall inside the 30-day minimum Foreign Visit Request processing window. For short-notice requirements, foreign military attachés must coordinate with their local sponsor to coordinate base access requirements. In regard to unofficial base access (leisure) outside of the NCR, foreign military attachés must pre-coordinate their visit with base security forces and foreign disclosure offices in advance of their visit. Installation access will be at the discretion of the installation commander.

9. Federal, State, and Local Law Enforcement, Investigative and Emergency Responder Credentials/Identification

a. The numerous credentials issued by various agencies makes it virtually impossible for security forces performing installation access control duties to know or determine visually if the credential is legitimate. This poses a significant risk to the installation with regard to this group of individuals accessing the installation by others posing as law enforcement, investigative, or emergency responder personnel, in addition to, introduction of unknown potential weapons or firearms onto the installation.

b. Law enforcement, investigative, or emergency credentials will not be routinely accepted as installation access credentials with exception of NCIS in accordance with reference (c). Installation commanders and directors may establish policy for use of law enforcement credentials that address the DoD Criminal Investigative Services for access consistent with this instruction and in accordance with references (c) and (af).

(1) NCIS agents who identify themselves using special agent credentials will be exempt from all routine searches of their persons, possessions, and materials, including their vehicles and occupants therein when accessing DON owned, controlled, or managed facilities or activities per reference (af).

(2) Individuals escorted by an NCIS special agent in the performance of official duties will not be required to present identification credentials.

c. Non-DoD federal agents will register the federal PIV when technologically feasible. When able to register, the PIV will be scanned by DBIDS as opposed to acceptance of law enforcement credentials.

d. Law enforcement, investigative, and emergency responder officials who do not have a DOD-issued CAC, a federally issued PIV, or if the installation cannot scan or verify the PIV, will be vetted in accordance with reference (c). After initial vetting, the person can be enrolled into the ePACS database by linking their driver's license as a credential, or they may be issued an LRC.

e. Acceptance will be based on support for special events and activities and only when acting in an official capacity.

f. For OCONUS DON installations and activities, United States credentialed persons with United States issued identification cards will be accepted. Any other form of authorized access will be under local agreement or treaty through the Department of State, regional, or installation commander.

g. Installations will develop/codify procedures for first responder installation access control during emergencies and authorized purposes (e.g. civilian law enforcement serving a warrant) in local guidance. These procedures should include alternate or pre-designated ACPs, to be used, if normal ACPs are congested or closed.

(1) During an emergency response, if notified by civilian authorities in advance, the senior installation security representative can waive basic requirements (identity proofing, fitness, purpose) for first responders responding to the emergency.

(2) Senior installation security representative will coordinate a plan with responding organizations that includes procedures for radio notification of emergency access before arriving at the ACP and incorporate procedures into civilian-military training scenarios.

(3) Installations should consider designating certain ACPs for use by in-bound emergency response vehicles, in the installation plan and training scenarios.

10. Unauthorized Access Reporting

a. Installation access control remains a high priority across the DoD and DON. Attempted and successful unauthorized installation access (also known as breaches or gate-runners) remains a significant threat to the physical security of DoD personnel and resources. Timely and accurate reporting and Root Cause Analysis (RCA) of all unauthorized access incidents is critical to evaluating trends, mitigating vulnerabilities, and developing effective solutions to counter potential threats.

b. Pursuant to reference (x), until otherwise directed, the Services will report all attempted and actual unauthorized installation accesses and all unauthorized overflights of United States installations by unmanned aerial systems on a monthly basis. DUSN (I&S) will compile and report to USD (I&S) as required.

c. Service and DON Component policy will require reporting of all unauthorized access events and a RCA reporting mechanism. The RCA should provide all information necessary to determine cause, evaluate trends, mitigate identified vulnerabilities, and develop effective solutions to counter future unauthorized accesses.

d. The following definition applies for DON reporting and RCA purposes:

(1) Attempted unauthorized installation access is defined as one or more individuals attempting to enter the installation without both completing the proper access control procedure and being granted access by security personnel, regardless of their intent.

(2) Successful unauthorized installation access is defined as one or more individuals proceeding past the final point at which they would be forced to stop, such as by a crash-rated vehicle or denial barrier at an ACP or by a perimeter fence or wall, regardless of their intent. Administrative stops, such as by a non-rated barrier or pursuing security

forces, are considered successful unauthorized installation access if they occur past the final point of forced stop.

(3) Unauthorized access. The act of a vehicle (manned or unmanned), aircraft, pedestrian, watercraft, or swimmer gaining access beyond the primary perimeter of a DON installation or special area without first being authorized to do so. For the reporting of an unauthorized access, the primary perimeter is defined as the ACP, perimeter fence, shore-line, within the area of Port Security Barrier (PSB) or established buoy-line. Additionally, unauthorized access is defined as:

(a) A vehicle that gains access past the vehicle turnaround area, final denial barriers, or established mitigation (e.g. blocking vehicle).

(b) An aircraft that crosses over restricted air space or lands on an installation or outlying field without prior authorization.

(c) A pedestrian that gains access to the installation by any means other than the established ACPs.

(d) A watercraft or swimmer that gains entry into the area protected by a PSB or established buoy-line, or accesses the installation via the shoreline.

DEVIATIONS, WAIVERS, AND EXCEPTIONS

1. Waivers and Exceptions. DON Services may request waivers or exceptions from minimum physical security requirements and standards if they specify and implement mitigating compensatory measures that provide equivalent or higher levels of protection. Permanent, or non-expiring, exceptions are not permitted.

2. Deviation Program. The Services will establish a deviation program to review and approve all conditions in which any subordinate commands or components are accepting a higher risk by deviating from minimum physical security requirements and standards. Exceptions approved by the Services will be reported to DUSN (I&S). Deviations to DoD policy that require DoD approval or have been delegated to the SECNAV or UNSECNAV for approval will be forwarded to the DUSN (I&S). Such requests require endorsement at the 3-Star level at a minimum from the Operational Commander and CNO/CMC levels. Service deviation programs will:

a. Establish procedures for waivers in the event of temporary deviations, less than one year.

b. Establish procedures for exceptions in the event of long-term deviations in excess of one year not to extend beyond three years.

c. Require documentation of waivers and exceptions and the threat, vulnerabilities, and risk involved in deviating from physical security minimum requirements and standards.

d. Require implementation and documentation of compensatory measures that provide an equivalent or greater level of protection as the standard requiring waiver or exception.

e. Designate a chain of command with responsibilities up to the Head of the DON Component to review and approve waivers and exceptions.

f. Require annual review by the chain of command of all waivers and exceptions and report annual updates to DUSN (I&S).

g. Prohibit granting of blanket waivers and exceptions across all locations or systems with a known deficiency and

require one waiver or exception for each occurrence of a deviation unless the head of the DON component has accepted the risk and issued a modification to a DON minimum standard.

h. Require the reporting of approved exceptions to DUSN (I&S) for follow on reporting to the Navy Security Enterprise Executive Committee, Defense Security Enterprise, and PSRB consistent with references (l) and (m).

3. Employment of the specific measures to mitigate a physical security vulnerability will be classified pursuant to the Original Classification Authority (OCA) Security Classification Guide (SGC) when risk and mitigation measures are combined together. Deviation requests which include specific measures will be classified pursuant to the OCA SCG. These measures include but are not limited to:

a. Navy and Marine Corps Security Forces and owner or user personnel.

b. MWD teams.

c. Physical barriers, facility hardening, and active delay or denial systems.

d. Secure locking systems, containers, and vaults.

e. ESS (e.g., IDS, radio frequency detectors, electronic emissions detectors).

f. Assessment or surveillance systems (e.g., closed-circuit television, thermal imagers, millimeter wave, radar).

g. Protective lighting (e.g., visible, IR).

h. Credential technologies, access control devices, biometrics, material or asset tagging systems, and contraband detection equipment.

i. Use of other research technologies being fielded under DoD programs.

ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

1. General. AA&E of all types are susceptible to theft. Certain military-unique AA&E, because they are unavailable on the commercial market and their potential to cause great numbers of casualties are particularly susceptible. All commanders and directors, therefore, must place special attention and emphasis on protecting AA&E. To reduce theft vulnerability and protection costs, commanders and directors must closely scrutinize the number and location of all firearms storage facilities on their installation with the goal of reducing and consolidating wherever possible consistent with operational, training, and safety requirements. Owners/users should only remove firearms from storage areas for as short a time as possible, and in as small a quantity as needed, to support specific missions or requirements.

2. The Heads of DON Services and Components possessing AA&E will:

a. Implement the procedures in reference (v) and develop supplemental guidance for the protection of AA&E in accordance with reference (w).

b. Oversee and develop written security policy that prescribes minimum physical security requirements for AA&E items not categorized Security Risk Category (SRC) I-IV and those items listed in reference (w) in subparagraphs 2.b.(2) through 2.b.(7).

(1) Copies of approved DON Component AA&E security policies for uncategorized AA&E (CAT-U) will be provided to DUSN (I&S) for routing to USD (I&S).

(2) DON Component AA&E security policies will prescribe minimum security requirements for weapon systems and platforms as described in reference (b).

c. Establish procedures to clearly define methods and requirements for accountability to include reporting of stolen, lost, or recovered AA&E in accordance with references (v), (w), and (z).

d. Exempt arms and ammunition issued to General and Flag Officers from the requirements in reference (v) (except for loss reporting), when appropriate. Where such exemptions are invoked, the affected arms and ammunition will be safeguarded and accounted for in a manner prescribed in policy by the heads of the DON Services and the minimum requirements outlined in enclosure (5) of reference (w).

e. Exempt arms and ammunition issued to specified DON component criminal investigators from the minimum standards outlined in reference (w) (except for loss reporting and the requirements outlined in enclosure (5) of reference (w) for personally retained weapons) if compliance would impede mission performance. Where exemptions are invoked, the affected arms and ammunition will be safeguarded and accounted for in a manner prescribed in policy by the heads of the DON Services and the minimum requirements outlined in enclosure (5) of reference (w).

f. Impose additional protective measures in addition to those prescribed in reference (w) where appropriate. Such measures will not violate or conflict with references (aa) and (ag).

g. Develop PSP that implement processes and procedures to assess and evaluate appropriate security measures based on continuous threat assessments, FPCON levels, physical security surveys and inspections, and vulnerability assessments. DON Components will also use risk management principles for mitigating, reducing, or eliminating risks. These programs must be threat-based, cost-effective, and include accountability and inventory control in accordance with references (v) and (w).

h. Plan, program, and budget requisite resources to protect AA&E in their possession and during transportation in accordance with the requirements in reference (w) and chapter 205 of reference (ah).

i. Accept AA&E shipments, at any time, for safe haven or after normal duty hours for secure hold as outlined in references (v) and (w).

j. Establish procedures for the review of all military AA&E storage facility construction, renovation, and modification projects in accordance with enclosure (5) of reference (w).

k. Establish procedures and coordinated response plans for accidents or incidents involving AA&E that include memoranda of understanding or agreements with non-DoD federal agencies in accordance with reference (ai).

l. Submit reports pertaining to mishaps involving AA&E in accordance with reference (ai).

m. Maintain a program to record, review, and track approved waivers and deviations from minimum AA&E physical and transportation security standards prescribed in this references (v) and (w).

n. Monitor solicitations and contracts involving SRC I-IV AA&E, listed in the appendix to enclosure (9) of reference (w), at contractor-owned contractor-operatored facilities for compliance with security requirements outlined in reference (w). Any additional requirements imposed by a DON-procuring command or activity will be specified in section H, "Special Clauses Section," of AA&E contracts. Additionally, the heads of the DON Components possessing AA&E will review:

(1) Solicitations and contracts for inclusion of entry authority to prime contractor and subcontractor facilities to enable the government to conduct security surveys, inspections, and investigations.

(2) Solicitations and contracts for inclusion of appropriate authority and contract clauses that apply to DoD AA&E in accordance with the appendix to enclosure (9) of reference (w).

(3) All contracts manufacturing A&E for compliance with the explosive safety requirements of reference (aj).

o. Coordinate with Director, Defense Counterintelligence and Security Agency after corrective actions have been taken by contract facilities or deviations are approved for contractor-owned contractor-operator facilities in accordance with reference (ag).

p. Identify a single office of record that will provide current information identifying its AA&E contractor and

subcontractor addresses, contract numbers, AA&E items and categories involved, and special protection requirements for all contractor locations where SRC I-IV are produced or stored.

q. Review physical inventories of AA&E in accordance with enclosure (8) of references (w) and (ak).

r. Include all protective measures outlined in reference (v) in Foreign Military Sales or Security Cooperation programs and contracts.

s. Ensure that shipments of AA&E are in accordance with enclosure (10) of reference (w) and chapter 205 of reference (ah).

ACRONYMS

AA&E	Arms, Ammunition, and Explosives
ACP	Access Control Point
ASN (EI&E)	Assistant Secretary of the Navy for Energy, Installations, and Environment
ASN (M&RA)	Assistant Secretary of the Navy for Manpower and Reserve Affairs
ASN (RD&A)	Assistant Secretary of the Navy for Research, Development and Acquisition
AVB	Active Vehicle Barrier
CAC	Common Access Card
CAF	Consolidated Adjudication Facility
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CONUS	Contiguous United States
DBIDS	Defense Biometric Identification System
DEERS	Defense Enrollment Eligibility Reporting System
DIR NCIS	Director, Naval Criminal Investigative Service
DHS	Department of Homeland Security
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DUSN (I&S)	Deputy Under Secretary of the Navy Intelligence & Security
ECP	Entry Control Point
ePACS	Electronic Physical Access Control System
ESS	Electronic Security Systems
FPCON	Force Protection Condition
GCC	Geographic Combatant Commander
GSA	General Services Administration
IMESA	Identity Matching Engine for Security Analysis
IDS	Intrusion Detection System
ISO	International Organization for Standardization
IT	Information Technology
ITO	Invitational Travel Orders
LRC	Local/Regional Credential
MWD	Military Working Dog
MWR	Morale Welfare and Recreation
NCIC	National Crime Information Center
NCIC III	National Crime Information Center Interstate Identification Index

NCIS	Naval Criminal Investigative Service
NCR	National Capital Region
OCA	Original Classification Authority
OCONUS	Outside the Contiguous United States
OSD	Office of the Secretary of Defense
PACS	Physical Access Control System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification-Interoperable
POW	Prisoner of War
PSB	Port Security Barrier
PSE	Physical Security Equipment
PSP	Physical Security Program
PSWG	Physical Security Working Group
RCA	Root Cause Analysis
SCG	Security Classification Guide
SDI&S	Senior Director for Intelligence & Security
SECNAV	Secretary of the Navy
SRC	Security Risk Category
TSDB	Terrorist Screening Database
TWIC	Transportation Workers Identification Credential
UAS	Unmanned Aerial System
UFC	Unified Facilities Criteria
UXS	Unmanned System
UNSECNAV	Under Secretary of the Navy
USD (I&S)	Under Secretary of Defense for Intelligence & Security
U.S.C.	United State Code
USCIS	United States Citizenship and Immigration Services
USG	United States Government
UUV	Unmanned Underwater Vehicle
UXS	Unmanned Systems
VCC	Visitor Control Center
VA	Department of Veterans Affairs
VHIC	Veteran’s Health Identification Card

DEFINITIONS

Unless otherwise stated, these terms and their definitions are for the purposes of this instruction.

1. Access Control. The process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances). A function or a system that restricts access to authorized persons only.

2. Access Control List. A list containing (at a minimum) the names of individuals authorized access and their subsequent authorities of sponsorship (e.g., privileges, times and/or dates for access, unescorted or escorted designation). In an electronic PACS, these items are logically stored in the PACS database.

3. ACP. Identified gap in an installation's perimeter security for pedestrian and/or vehicular access contained within an Entry Control Point.

4. Access Credential. A physical artifact issued by the federal, state, or local government that attests to one's right to credit or authority. The access credential contains and/or depicts characteristics, authorizations, and privileges for physical access and internal security controls.

5. AVB. A barrier generally used at critical ACP. Active barriers have moveable parts, some of which, or most all of the parts, are power assisted. The systems are manually or mechanically operated to allow or prevent vehicles passing through.

6. Ammunition. A device charged with explosives, propellants, and pyrotechnics, initiating composition, riot control agents, smoke, and flame for use in connection with defense or offense, including demolition. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or

having unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition, and rim-fire ammunition are excluded.

7. Applicant. An individual requesting physical access to a facility and/or installation.

8. Application. A hardware and/or software system implemented to satisfy a particular set of requirements.

9. Arms. A weapon that will or is designed to expel a projectile or flame by the action of the explosive, and the frame or receiver of any such weapon.

10. Asset. Any DON resource that merits protection and includes but is not limited to: installations, facilities, aircraft, vessels, and AA&E in accordance with references (f) and (g).

11. Authentication. A process that matches presented information to the established origin of that information. The process of establishing confidence of authenticity, and in the validity of a person's identity, and the PIV card.

12. Biographic Information. Facts that assert or support the establishment of an individual's identity. The identity of United States citizens is asserted by their social security number and given name. Other biographic information may include, but is not limited to, identifying marks such as tattoos, birthmarks, etc.

13. Biometrics. A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. An authenticator produced from measurable qualities of a living person.

14. Commanders/Director. Personnel assigned to command positions at all levels and the heads of the Defense Agencies and DoD Field Activities.

15. Controlled Area. A controlled space extending upward and outward from a specified point. Installations are generally

considered controlled areas for the purposes of national defense. Commanders and/or directors may further designate controlled areas within an installation based upon geographic attributes and unit dispersal. Controlled areas generally designate areas wherein sensitive operations occur or controlled unclassified and sensitive information is stored and access is limited to specific persons.

16. Credential. A physical artifact such as a PIV card or a data object such as a digital certificate that provides evidence of a person's approval for physical or logical access.

17. Deviation. Inability to achieve a minimum physical security standard for facilities, equipment, and procedures either combined or individually.

18. Exception. An approved exclusion from a standard or requirement or continuation of a non-standard condition that creates vulnerability and requires compensatory measures.

19. DoD Installation. Military installations and stand-alone DoD facilities, agencies, or buildings not on military installations.

20. DoD Issued Card. Cards (other than the DoD CAC) issued by a component of the DoD.

21. Entry Control Facility. Encompasses the overall layout, organization, infrastructure, and facilities associated with an access point.

22. ECP. An internal access control portal to a building or building compound once one passes through an existing installation ACP.

23. Escorted Individuals. Persons who require access, without determination of fitness, who must be accompanied by a sponsor with authorization to escort the individual. The escort requirement is mandated for the duration of the individual's visitation period.

24. Explosives. Any chemical compound, mixture, or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to: individual land mines,

demolition charges, blocks of explosives (dynamite, trinitrotoluene, C-4, and other high explosives), and other explosives consisting of 10 pounds or more (e.g., gunpowder or nitro guanidine).

25. Federal PIV. A physical artifact issued by the Federal Government to an individual that contains a photograph, cryptographic keys, and a digitized fingerprint representation so that the claimed identity of the card holder can be verified by another person (human readable and verifiable) or a computer system readable and verifiable. This card conforms with the standards prescribed in reference (c).

26. Fitness. Level of character and conduct determined necessary for the basis of access control decisions.

27. Identity Proofing. The process of providing sufficient information (e.g., identity history, credentials, or documents) to a registrar when attempting to establish an identity based on a review of authorized and acceptable documentation as outlined on a DHS Form I-9.

28. Installation. Real DoD properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor and USG operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

29. Interoperable. Allows any government facility or information system, regardless of the PIV or PIV-I issuer, to electronically verify a cardholder’s identity using the credentials on the PIV card.

30. Interoperability. The ability of any government facility or information system, regardless of the PIV or PIV-I issuer, to verify a cardholder’s identity using the credentials on the PIV or PIV-I card.

31. Logical Access. Use of a credential to access IT systems.

32. Perimeter Control. Includes objects and measures deployed to establish physical boundaries such as barriers, vehicle barriers, fences, natural barriers.

33. Physical Access. Vehicle and pedestrian access to DON- or federally-controlled installations, facilities, and other locations. Access may be unescorted or escorted.

34. Physical Access Control. The process of physically controlling personnel and vehicular entry to installations, facilities, and resources or contact with controlled materials. Access will be either unescorted or escorted.

35. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

36. PII. PII is information that can be used to distinguish or trace an individual's identity, such as their 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 specific individual.

37. PIV Card. A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, and digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

38. PIV-I Card. Personal identity credentials issued by DoD-approved non-federal issuers that have the DoD-approved vetting, validation, and revocation processes in place as part of their issuance procedures, and have been certified by GSA as passing all policy and testing requirements under the GSA Certification and Accreditation Program for non-federal issuers.

39. Restricted Area. An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized

by the installation or activity commander or director, posted, and will employ physical security measures.

40. Risk. A measure of consequence of peril, hazard, or loss, which is incurred from a capable aggressor or the environment (probability and severity of loss linked to threats or hazards).

41. Screening. The physical process of reviewing a person's presented biographic and biometric information, as appropriate, to determine their authenticity, authorization, and credential verification against an approved data source through authorized and secure channels any time during the person's period of physical access eligibility. This assessment identifies derogatory actions that can be determined as disqualifying issues for current or continuing physical access eligibility standards and requirements for the resource, asset, or installation.

42. Security Force. Personnel at an installation or facility who are tasked to provide physical security, force protection, or law enforcement.

43. Threat. The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.

44. Unescorted Individuals. Personnel who have been identity proofed and favorably vetted for unescorted access within the installation; but who are, however, still subject to any controlled or restricted area limitations, as appropriate.

45. Vetting. An evaluation process of an applicant's or card holder's character and conduct for approval, acceptance, or denial for the issuance of an access control credential or physical access. For PIV-I credentials, this includes an approved vetting process for the organizational entity as well as the applicant, or card-holder, being sponsored by that entity.

46. VHIC. A card issued by the VA. The card is primarily used at VA medical facilities and issued only to eligible veterans for VA medical benefits. The card displays the veteran's name, picture, and special eligibility indicators (e.g., Service

Connected, Purple Heart, and Former POW) on the front of the card, if applicable.

47. Vulnerability. A situation or circumstance, which left unchanged, may result in loss of life or the degradation of or damage to installations, missions, and assets.

48. Waiver. A temporary condition that deviates from an established physical security standard and requires compensatory measures.