STANDARD OPERATING PROCEDURE
Security Services Division
Visitor Management Branch

ACCESS CONTROL CENTER (ACC)
STANDARD OPERATING PROCEDURES

May, 2021

Distribution Statement E: Distribution authorized to DoD Components only (Administrative or Operational Use) (July 2008). Other requests for this document shall be referred to the Security Services Directorate (SSD) of the Pentagon Force Protection Agency.

THIS PAGE LEFT INTENTIONALLY BLANK

Table of Contents

Pentagon Force Protection Agency
Security Services Division

1. INTRODUCTION.

The Pentagon Force Protection Agency (PFPA) is responsible for providing law enforcement, force protection, and security services for the Pentagon Reservation; assigned designated Department of Defense (DoD) facilities within the National Capital Region (NCR), and DoD activities in the NCR. One of PFPA's key missions is to ensure all DOD employees are authorized to access and work in areas approved for processing and storing classified national security information. The PFPA Access Control program is one of multiple tools at PFPA's disposal to protect sensitive information and other DOD assets.

Access Control Center
Standard Operating Procedures

SUBJECT: Standard Operating Procedures for the Access Control Center (ACC)

REFERENCES:

1) Department of Defense (DoD) Manual 5200.01, Volume 3, DoD Information Security Program: Overview, Classification, and Declassification
2) DoD Manual 5200.01 Volume 1, Information Security Program, Updated 2018
3) DoD Manual 5200.40, Information Technology Security Classification and Accreditation Process
4) DoD Manual 5220.22-M, National Industrial Security Program Operating Manual
5) DoD Directive 5105.68, Pentagon Force Protection Agency (PFPA)
6) Director of Administration and Management Administrative Instruction (AI) No. 30, *Incorporating Change October, 2019,* Force Protection on the Pentagon Reservation (PFPA)
7) Director of Administration and Management Administrative Instruction (AI) No. 88, August 26, 2009, Pentagon Reservation Vehicle Parking Program
8) Intelligence Community Directive (ICD) No. 703, Protection of Classified National Intelligence Including Sensitive Compartmented Information,
9) ICD No. 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,
10) ICD No. 705, Sensitive Compartmented Information Facilities, (Version 1.5 2020)

1. PURPOSE

The purpose of this Pentagon Force Protection Agency (PFPA) Standard Operating Procedure (SOP) is to outline the administrative procedures, responsibilities, and duties for the Access Control Center. These procedures provide instructions for the daily services provided to customers concerning access control within the National Capitol Region (NCR). This is a fluid document and changes may be made on a continual bases.

2. RESPONSIBILITIES

2.1. Director, Security Management.

2.1.1. The Director, Security Management is responsible for security operations as they relate to PFPA's mission to protect personnel, infrastructure and critical assets at the Pentagon and protected facilities.

2.1.2. Provides qualified and trained security specialists to accomplish physical security and access control duties in support of the Agency's mission.

2.2. Director, Security Services.

2.2.1. The Director, Security Services Division is responsible for Credentialing and Visitor Management operations at the Pentagon and Mark Center.

2.2.2. Responsible for all operations relative to access control.

2.3. Chief, Visitor Management Branch: Oversees Visitor operations at the Pentagon and Mark Center and Access Control Center operations.

2.4. ACC Senior Office Manager.

2.4.1. Provide office management, prioritizes access requests and develop policies and procedures to maintain mission efficiency.

2.4.2. Assists Credentialing Office in CAC/PFAC issuance, proximity/swipe privilege and PIN requests.

2.5. ACC Administrative (Assistant): Responsible for processing access request and photo permits and database management.

3. PROCEDURES

3.3. Security Manager Appointment Letters/Memorandums (per Title 32, Part 234, Section 15, Code of Federal Regulations)

3.3.1. Security Manager Appointment Letters will be emailed to: **PFPA SSD Mailbox**

3.3.2. Activity Security Manager Appointment memos shall be signed by the Head of the Activity (illustrated in figure 1.1).

3.3.3. Assistant Security Manager and Security Assistant appointment memos must be digitally signed by the Activity Security Manager and include everything provided in the example (illustrated in figure 1.2).

3.3.3.1. Operational Hours and Classification: The Security Manager shall ensure that changes to operating hours and / or classification for alarmed spaces are immediately coordinated with the ACC via an updated memo. This is for ACC documentation purposes and coordination with the Pentagon Operations Center for appropriate response.

3.3.4. All Security Managers must have a memo on file with the ACC that is compliant with DoDM 5200.01, Volume 1

3.3.5. Security Managers shall first establish their respective appointment memos before submitting PFPA form 79s.

3.3.6. All new Security Managers are required to schedule an orientation briefing with the ACC.

3.3.6.1. Within 5 business days of their appointment.

3.3.6.2. Security Managers shall send an Outlook meeting invite to the Appointment-Letter workflow mailbox.

3.3.6.3. This brief takes around 10 minutes and we can schedule a briefing from 09:00 am to 09:30 am or 2:00 pm to 2:30 pm on Tuesdays pending any previous engagements. Alternate dates and time, can be made by contacting our office at 703-614-1529.

3.3.6.4. Due to the Covid-19 pandemic, the ACC has temporarily discontinued conducting on-site Security Manager Briefings. Instead, new incoming security managers are given the below listed documents and PowerPoint via email to thoroughly review.

3.3.6.4.1. 5200.01 (pages 28-31)

3.3.6.4.2. PFPA Form 79 (blank)

3.3.6.4.3. Security Do's & Don't

3.3.6.4.4. New Security Manager PowerPoint Slides

3.3.6.4.5. PFPA Arm/Disarm Instructions

3.4. Routine request: Under 20 personnel requests will take two (2) business days to fulfill, and the sender will receive an email once it has been completed. Routine request will be accessed using: **PFPA SSD Mailbox**

3.5. Expedite Request: For SES, General Officers, or an articulated emergency situation, security managers may request a (1) business day expedite request using PFPA Form 79 for the spaces that they are responsible for. The sender will receive an email once it has been completed. Requests will be accessed using: **PFPA SSD Mailbox**

3.6. Bulk Request: When requesting access for 20 or more personnel to an alarmed room or space, the Form 79 is required to be filled out in its entirety for all personnel requiring access.

3.7. Existing Rosters

3.7.1. Additions/Deletions: The Activity Security Manager, Assistant Security Manager, or Security Assistant shall submit requests through the Access Management Portal (AMP).

3.7.2. Upon the removal of an employee from a secured space, the Activity Security Manager, Assistant Security Manager, or Security Assistant must submit a roster highlighting all individuals that need to be deleted from a specific space(s) to the Access Control Workflow Mailbox.

3.8. Pentagon Perimeter Access: The ACC will support credentialing branch for perimeter request on a needed basis. (illustrated in figure 1.4).

3.9. Parking Management Program

3.9.1 Secure Parking Reader Group – upon receipt of a VIP parking permit, the WHS Parking Management Office will request access for VACPs.

3.9.2 By nature of having the Secure Parking Reader Group, VIP parkers will also receive the adjacent turnstiles / gates.

3.10. Arming / Disarming instructions (illustrated in 1.5)

3.11. Mirroring Request- The ACC will NOT process "mirror requests" (copying access from an individual's CAC to another individual(s) CAC).

3.12. Extent of troubleshooting faulty access

3.12.1. View profile to verify access
3.12.2. If access has been verified then ACC will re-download access
3.12.3. After 15 minutes, if access still does not work, the customer will be referred to ISSC Contractor for additional troubleshooting.

3.13. History Request

3.13.1 History Request may be sent via e-mail from the Activity Security Manager, Assistant Security Manager, or Security Assistant to the Access Control Workflow Mailbox.
3.13.2. Must include a valid reason in the e-mail.
3.13.3. History Requests are not be used for timesheet verification, attendance confirmation, or any other administrative action other than those associated with security.

3.14. Swipe History Information Request – Handled exclusively by PFPA/SSD Management (illustrated in figure 1.6)

3.14.1. Security Manager, Law Enforcement, or Intelligence personnel will submit their initial request for employee swipe history to the PFPA Security Services Division (SSD), expedite workflow mailbox.
3.14.2. The ACC Physical Security Specialist will email a blank swipe history report form to the requesting Security Manager, Law Enforcement, or Intelligence personnel.
3.14.3. The requesting personnel will send the completed Swipe History Information Request form back to the expedite mailbox.
3.14.4. The report form is screened for completeness and then submitted to authorizing official for final approval.
3.14.5. Upon final approval, a case number is assigned and documented on the swipe history log sheet located on the PFPA O: Drive.
3.14.6. The report form is submitted to the Network Control Center (NCC) for processing.
3.14.7. Once completed, the ACC will check the swipe history report for completeness and/or possible inconsistencies.
3.14.8. The swipe history report is submitted to the requesting Security Manager, Law Enforcement, or Intelligence personnel with the case number for reference.
3.14.9. All reports and email communications are saved to the PFPA O- Drive:
3.14.10. As with all expedite request, there is a projected 24 hour turnaround time. Unless impacted by unforeseen circumstances outside of the ACC's immediate control.
3.14.11. If the original request needs to be edited or modified in any way, a new

request will need to be submitted with the changes reflected on the report form.

3.14.12. The Chief of Visitor Management Branch has delegated authority to Approve "Swipe History Information Request" on behalf of the Director of Security Management.

3.15. Photo Permits (per Title 32, Part 234, Section 15, Code of Federal Regulations)

3.15.1. Shall be processed upon receipt of two statements of understanding and signed request form.

3.15.2. An incomplete photo permit knowledge package will not be accepted.

3.15.3. The entire "Consolidated Photo Credentials Request Packet --- 2019" (illustrated in figure 1.7) needs to be emailed by the security manager to the Photo Permit Workflow Mailbox at: **PFPA SSD Mailbox**

4. At least annually, the ACC Senior Office Manager should ensure that procedures documented in this standard operating procedure are being followed. On an annual basis, audits will be conducted and the audit results will be made available in the form of a signed memorandum to the Director SSD and/or Deputy Director SSD. All personnel are responsible for reporting violations of this SOP to their branch chief within 24 hours.

5. GLOSSARY AND ABBREVIATIONS

5.1. Glossary

5.1.2. **Activity Security Manager** – The individual specifically designated in writing and responsible for the activity's information security program, which ensures that classified information (except SCI (Sensitive Compartmented information) which is the responsibility of the SSO (Special Security Office) appointed by the senior intelligence official) and CUI (Controlled Unclassified information) are properly handled during their entire life cycle.

5.1.3. **Assistant Security Manager** – In large activities and where circumstances warrant, activities may designate U.S. Government civilian or military members as assistant security manager(s) to assist the activity security manager with program implementation, maintenance, and local oversight.

5.1.4. **Heads of DoD Activities** – Heads, either military or civilian, of organizations, commands, and staff elements subordinate to a DoD Component, with jurisdiction over and responsibility for the execution of the organization's mission and functions, including its information security program. The official may carry the title of commander, commanding officer, or director, or other equivalent title.

5.1.5. **Perimeter Door** - A pedestrian or vehicle portal providing ingress or egress to the building's Access Zone.

5.1.6. **Mirror Request** – The unauthorized copying of access from one or more individual(s) profile in order to paste into another individual(s) profile.

5.1.7. **Security Assistant** - As warranted, activities may assign U.S. Government civilian, military members, or contractor employees as security assistants to perform administrative security functions under the direction of the activity security manager without regard for job series or title or for rank, rate, or grade as long as they have the clearance required for the access needed to perform their assigned duties and tasks.

5.1.8. **Special Purpose Perimeter Door** - An unmanned perimeter door with any form of networked and monitored access control allowing ingress or egress.

5.1.9. **Turnstile** – any of the pedestrian gates adjacent to each VACP.

6.1. **Abbreviations**

ACC – Access Control Center
ACS – Acess Control System
AMP – Access Management Portal
ASM – Activity Security Manager
Asst. SM – Assistant Security Manager
IDS – Intrusion Detection System
PDWG – Perimeter Door Working Group
PFPA – Pentagon Force Protection Agency
POC – Pentagon Operations Center
PPD – Pentagon Police Department
SA – Security Assistant
SSD – Security Services Division
VACP – Vehicle Access Control Point