**U.S. Department of Agriculture (USDA) Office of Homeland Security and Emergency Coordination (OHSEC) Physical Security Division (PSD)**

**Physical Security Assessment Template (PSAT)**

The U.S. Department of Homeland Security (DHS) Interagency Security Committee (ISC) standards require that physical security assessments of occupied, Level 1 facilities must be conducted every 5 (five) years. These standards establish a baseline for physical security countermeasures to be applied to all Federal facilities and provide the framework for the customization of security countermeasures to address unique risks at a facility. This baseline is used to identify vulnerabilities in all five areas of physical security, including site, structural, entrances, interior, security systems, and security operations and administration.

Under 7 Code of Federal Regulations (CFR) 2.95 b (7) and in support of the Secretary's Strengthening Services Administrative Solutions (SSAS), the USDA Office of Homeland Security and Emergency Coordination (OHSEC) Physical Security Division (PSD) is tasked and has conducted over 70 physical security assessments over the past eighteen months. The OHSEC PSD utilizes the Government Accountability Office (GAO) approved Risk Based methodology in the conducting physical security assessments. This expertise was utilized in creating training and additional guidance to inform and educate employees. Throughout these assessments, common vulnerability trends were encountered.

- Lack of Facility Key Control
- Absence of notification for employees when visitors enter the facility
- Janitorial staff works after core business hours, has key access to facility and does not have a background check completed
- Server room doors are left open due to insufficient temperature control
- Windows on ground level are being left unsecured with blinds and shades not being drawn at night
- Areas/rooms/cabinets containing Personal Identifiable Information (PII) are not properly secured
- Lack of card readers for computers which prohibits an employee from accessing their computer with their LincPass

Each identified threat to a facility creates a vulnerability that should be mitigated. The risks to the facility could vary based on geographical location, type of facility and work environment.

In an additional proactive effort to meet these standards, USDA has created the PSAT Program; designed to increase the ease and efficiency of completion of required physical security assessments. The program provides security, as well as non-security professionals, the resources necessary to identify current vulnerabilities at their facilities. PSAT will not only provide compliance with established ISC standards, but will also provide a significant cost savings. Components of the program include a self-assessment tool, training materials, security reports capabilities, security analyst resources and mitigation recommendations. This report could also be leveraged as a justification in requesting funds within the budget cycle for any recommendations that require additional funding.

**Physical Security Assessment Template**
**USDA Service Center**
(V7.7 11/26/2013)

**Instructions:**

For Yes/No choices, please select one (1) option that best satisfies the question. Please feel free to add a brief explanation to any question in this assessment.

For questions with multiple choices, select all that apply to the question, or "NONE/NEVER" if no choices apply. You can also submit additional items to an answer using the "OTHER" choice.

## I. Facility Background Information

**Complete the following facility information.**

- Facility Name (i.e. Fredericksburg, VA Service Center):
- Facility Street Address:
- Facility City:
- Facility State:
- Facility Zip Code:
- Point of Contact Name:
- Point of Contact Agency:
- Point of Contact Title:
- Point of Contact Phone Number: ( ) -
- Point of Contact Email Address:
- Date Assessment Was Completed: Click here to enter a date.

*If a security assessment has been performed at this site before, list the date of the assessment (excluding FSA-774, FSA-780 and FSA-781 assessments). Additional information and attachments can be provided in the final section.*

- Date of last assessment: Click here to enter a date.

## II. Service Center Facility Information

**1. What is the ownership type for this facility?**
☐ USDA Owned/Leased
☐ Agency Commercial Lease
☐ GSA Owned/Leased
☐ Other Agreement

**2. If leased, does your current lease expire in less than two years?**
☐ Yes
☐ No

3. **Is this Service Center occupied with another Federal or USDA Service Center Agency?**
   - ☐ None
   - ☐ Farm Service Agency (FSA)
   - ☐ Rural Development (RD)
   - ☐ Natural Resources Conservation Service (NRCS)
   - ☐ Soil and Water Conservation District
   - ☐ County Office
   - ☐ Other (explain):

4. **Are there any other tenants that reside in your same facility? (i.e. Doctor's Office, Restaurant, etc.)**
   - ☐ Yes (explain):
   - ☐ No

5. **Select from the below options which best describes the type of area in which this facility is located.**
   - ☐ Rural (outside City limits)
   - ☐ Urban
   - ☐ Suburban
   - ☐ Strip Mall
   - ☐ Close to international border
   - ☐ GSA Federal Building
   - ☐ Other (explain):

6. **What is the rentable square footage within the Service Center?**
   Square Footage:

7. **What year was this building constructed?**
   Year:

8. **What type of construction is this building? (Select all that apply)**
   - ☐ Single-story
   - ☐ Multi-story
   - ☐ Standalone
   - ☐ Adjacent to other buildings
   - ☐ Other (explain):

9. **What is the primary exterior construction material for this building? (Select all that apply)**
   - ☐ Concrete
   - ☐ Masonry
   - ☐ Steel
   - ☐ Wood
   - ☐ Other (explain):

10. **Are there any window air conditioning units installed on the first floor or basement level?**
    - ☐ Yes
    - ☐ No

11. **If yes, are they protected with a cage on the exterior of the building?**
    - ☐ Yes
    - ☐ No

12. **Do you believe you have adequate lighting at the entrance and in parking areas at night? (i.e. Do employees feel safe walking to vehicle areas or exits after dark?)**
    - ☐ Yes
    - ☐ No (explain):

13. **Is the landscaping maintained in a manner which allows adequate visibility from the street? (i.e. Is shrubbery and landscaping not overgrown, which if it is can provide a hiding place for an intruder?)**
    - ☐ Yes
    - ☐ No (explain):

14. **Is mail delivered to a mailbox located within the Service Center?**
    - ☐ Yes
    - ☐ No (explain):

15. **Does the Janitorial Service have a key to the Service Center?**
    - ☐ Yes
    - ☐ No
    - ☐ N/A

16. **Have the Janitorial Service employees undergone a background investigation that has been verified by the Government?**
    - ☐ Yes
    - ☐ No
    - ☐ N/A

17. **How many of the following employees work at this Service Center:**

| Number of Employee Types | FSA | RD | NRCS | Total |
|---|---|---|---|---|
| FTE Federal Employees (includes FSA county employees) | | | | |
| Temporary Employees | | | | |
| Volunteers | | | | |
| Seasonal Employees | | | | |
| Contractors | | | | |
| County Employees (paid by county) | | | | |
| State employees | | | | |
| Soil and Water Conservation District | | | | |
| Other: | | | | |

## III. Emergency Response/Preparedness

**18. What is the average local Fire Department/Emergency Medical Service (EMS) response time to the Service Center?**

- ☐ Less than 15 minutes
- ☐ 15 – 30 minutes
- ☐ More than 30 minutes
- ☐ Other (explain):

**19. What is the local Police Department response time to the Service Center?**

- ☐ Less than 15 minutes
- ☐ 15 – 30 minutes
- ☐ More than 30 minutes
- ☐ Other (explain):

**20. Does the local Police Department actively patrol your area?**

- ☐ Yes
- ☐ No
- ☐ Unknown

**21. Who is the Law Enforcement agency that is responsible for investigating crime at your facility?**

- Law Enforcement Department:
- Non-Emergency Phone Number: (  )  -

**22. Is the Fire department familiar with your facility? If yes, how?**

- ☐ Yes (explain):
- ☐ No

**23. How often does the Fire Department conduct site inspections?**

- ☐ Quarterly
- ☐ Monthly
- ☐ Annually
- ☐ Semi-Annually
- ☐ Never

**24. What type of fire prevention and notification systems are used in this building?**

- ☐ None
- ☐ Sprinkler System
- ☐ Fire extinguishers
- ☐ Smoke Alarms that have batteries changed annually or semi-annually

**25. Does the facility have an updated Occupant Emergency Plan (OEP)/Emergency Occupant Plan (EOP)?**

- ☐ Yes
- ☐ No

**26. Is there a plan in place or a "safe word" to be used to notify employees of an irate customer or threatening situation?**

- ☐ Yes
- ☐ No

## IV. Facility Entrance/Exit Points

**27. Is there a procedure in place to ensure the Service Center is always secured after hours or when employees are not in the facility?**

- ☐ Yes
- ☐ No (explain):

**28. Other than the main entrance, are all other facility entrances secured at all times? (i.e. employee side entrance or emergency exits)**

- ☐ Yes
- ☐ No (explain):

**29. What is used to secure the main entrance door? (Select all that apply)**

- ☐ None (unsecured)
- ☐ Lock and key
- ☐ Keypad
- ☐ Electronic Card Reader
- ☐ Guard
- ☐ Deadbolt
- ☐ Other (explain):

**30. What is used to secure all other entrance doors? (Select all that apply)**

- ☐ None (unsecured)
- ☐ Lock and key
- ☐ Keypad
- ☐ Electronic Card Reader
- ☐ Guard
- ☐ Other (explain):

**31. What type of entrance door is on the main entrance of the Service Center?**

- ☐ Metal
- ☐ Solid Core Wood
- ☐ Hollow Core Wood
- ☐ Glass
- ☐ Other (explain):

**32. Are the building windows closed and locked after normal duty hours?**

- ☐ Yes
- ☐ No
- ☐ Other - Windows are non-operable (cannot open)

**33. Are first floor blinds closed after normal duty hours?**

- ☐ Yes
- ☐ No
- ☐ Windows are tinted
- ☐ No blinds installed

**34. Are there any access points on the roof that could provide illegal entry into the service center?**

- ☐ Yes
- ☐ No

**35. If yes, are they secured?**

- ☐ Yes
- ☐ No

## V. Security Measures

**36. What type of security measures are in place to protect assets, including employees and visitors, inside the building? (Select all that apply)**

- ☐ None
- ☐ Protected customer service counter (i.e. Barrier to keep visitors on public side of office)
- ☐ Entrance door chime
- ☐ Duress alarm button
- ☐ Video Surveillance
- ☐ Intrusion Detection System (IDS) on doors
- ☐ IDS on windows
- ☐ Motion Sensors in hallways
- ☐ Motion sensors on perimeter lights
- ☐ Other (explain):

**37. How does the alarm monitoring system annunciate when an event occurs? (Select all that apply)**

- ☐ None
- ☐ Pages designated personnel
- ☐ Notifies monitoring center who then phones designated personnel, police, fire, or EMS
- ☐ Contacts police, fire, or EMS directly
- ☐ Not applicable
- ☐ Other (explain):

**38. What are the facility visitor management procedures? (Select all that apply)**

- ☐ None
- ☐ Check in at front desk
- ☐ Sign in/sign out sheet
- ☐ Issue visitor site badge
- ☐ Government ID (LincPass)
- ☐ Escorted
- ☐ Other (explain):

**39. Are the main electrical panels and phone service boxes locked or located in a secure room? (i.e. Tamper proof lock)**

☐ Yes
☐ No

**40. Does your facility have a key custodian for all keys/badges?**

☐ Yes
☐ No

**41. Are the keys 100% inventoried annually?**

☐ Yes
☐ No (explain):

**42. Is a log book used when issuing keys?**

☐ Yes
☐ No
☐ Other (explain):

**43. Have your office door locks been rekeyed in the past ten years?**

☐ Yes
☐ No

**44. Are Personal Identification Numbers (PINS) reset on cypher locks, card readers, and combination locks when an employee is no longer employed by the office?**

☐ Yes
☐ No
☐ N/A

**45. Do you have a written Standard Operating Procedure (SOP) to retrieve keys and LincPasses from terminated employees?**

☐ Yes
☐ No

**46. Does your facility have cross-cut shredding capabilities for sensitive documents?**

☐ Yes
☐ No

**47. Do all personnel in the Service Center, who are authorized, possess a LincPass? If no, please explain.**

☐ Yes
☐ No (explain):

**48. Do all personnel with an issued LincPass use the credential to access their computer during performance of their daily duties? If no, please explain.**

☐ Yes
☐ No (explain):

## VI. Working in Field/Remote Work

**49. Indicate which agencies have employees who leave the facility to perform work in remote locations? (i.e. on farms or ranches)**

**FSA**
☐ Yes
☐ No (explain):

**RD**
☐ Yes
☐ No (explain):

**NRCS**
☐ Yes
☐ No (explain):

**50. Indicate which agencies have employees who receive training that pertains to work performed in remote locations? (i.e. tactical situational awareness training, self-defense courses) If yes, please explain.**

**FSA**
☐ Yes
☐ No (explain):

**RD**
☐ Yes
☐ No (explain):

**NRCS**
☐ Yes
☐ No (explain):

**51. Indicate which agencies have staff that provides an itinerary of field locations prior to heading into the field?**

**FSA**
☐ Yes
☐ No (explain):

**RD**
☐ Yes
☐ No (explain):

**NRCS**
☐ Yes
☐ No (explain):

**52. Indicate which agencies have employees who usually accompany each other when working in remote locations? If no, please explain.**

**FSA**
☐ Yes
☐ No (explain):

**RD**
☐ Yes
☐ No (explain):

**NRCS**
☐ Yes
☐ No (explain):

**53. How does the facility maintain communication with employees working in remote locations?**
☐ Not applicable
☐ None to Partial coverage
☐ 2-way radio
☐ Personal Cell phone
☐ Government Cell phone
☐ Other (explain):

**54. How are your Government vehicles secured at the facility? (i.e. locked when not in use)**
☐ Locked when not in use
☐ Locked behind fence when not in use
☐ Unlocked when not in use
☐ Other (explain):

**55. Are Government vehicle keys and Fleet Charge Cards secured when not in use? (i.e. locked in a key box, cabinet, or desk)**
☐ Yes
☐ No

**56. How are Government vehicle license plates affixed to each vehicle?**
☐ Philips Head or Flat Head Screws
☐ Bolts
☐ Security Screws
☐ Other (explain):

## VII. <u>Criminal Activity (Threats)</u>

**57. Have any security incidents occurred at the facility in the past 2 years. If yes, please enter the number of incidents as well.**
☐ Yes (explain):
☐ No

58. **Have any criminal incidents occurred, in the area where an employee was performing field work? If yes, please explain.**
☐Yes (explain):
☐No

59. **Are there any high risk areas, such as, correctional facilities, drug rehabilitation facilities, homeless shelters, transient areas (railroad yards, homeless populations) or transportation hubs (bus stations) in the surrounding area? If yes, please explain.**
☐Yes (explain):
☐No

## VIII. Asset Classification

60. **Identify the facility assets that are critical to the organization's mission from the list below, enter "N/A" for non-applicable assets. Specify if each asset is securely stored or not. For assets not securely stored, please explain below:**

| Assets | List Critical Assets | Securely Stored? (yes/no) If no, please explain. |
|---|---|---|
| Legal documents (e.g. agreements, Farm Bill contracts, deeds) | | ☐Yes<br>☐No(explain): |
| Financial documents (e.g. checkbook, Tax forms) | | ☐Yes<br>☐No(explain): |
| Desktop and Laptop computers | | ☐Yes<br>☐No(explain): |
| Communication Devices (e.g. 2-way radio) | | ☐Yes<br>☐No(explain): |
| Government Fleet Vehicles | | ☐Yes<br>☐No(explain): |
| Other (explain): | | ☐Yes<br>☐No(explain): |

61. **How are vital and sensitive hardcopy documents secured in the facility? (i.e. PII) (Select all that apply)**
☐Not Applicable
☐Unsecured storage (e.g. unlocked filing cabinet)
☐Locked storage
☐Fireproof storage
☐Waterproof storage
☐Backed up on server (e.g. PDF files)
☐Other (explain):

## IX. IT Infrastructure Security (Can be completed with the assistance of ITS, if necessary.)

62. **Are laptop computers, at the facility, physically secured? (i.e. cable locks)**
☐Yes

☐ No

**63. List all IT assets located in the server room? (i.e. mail server, router, switch, etc.)**

**64. Has an access list been developed and maintained for both authorized unaccompanied and accompanied access to the server room? If no, skip question 65.**

☐ Yes
☐ No

**65. For the accompanied access list, which of the following are depicted on the sign-in sheet? (Select all that apply)**

☐ Name
☐ Organization
☐ Signature
☐ Type of ID used for proof of Identity
☐ Date and time of access and departure
☐ Purpose of visit
☐ Other

**66. Is there an Uninterruptable Power Supply (UPS) designated to the servers to allow for timely shutdown of the system in cases where commercial power is lost?**

☐ Yes
☐ No

**67. Is power equipment and IT infrastructure outside the facility properly protected? (i.e. bollards to prevent a vehicle from accidently running into the infrastructure)**

☐ Yes
☐ No

**68. Are there any water sources within the immediate area that would cause damage to the IT equipment if compromised?**

☐ Yes
☐ No

**69. Is there emergency lighting in the server room?**

☐ Yes
☐ No

**70. What type of access control system is used to enter the server room inside the building? (Select all that apply)**

☐ Not Applicable
☐ Unsecured door
☐ Key Lock
☐ Electronic Card Reader

**71. Is there an astragal over the server room key lock? (An astragal or anti-pick plate protects against someone sliding a tool into the locking mechanism for easy compromise.)**

☐ Yes

☐ No (explain):

**72. What types of security measures are in place to protect the server room inside the building? (Select all that apply)**

☐ Door secured at all times
☐ Sign in/sign out sheet
☐ Reinforced wall construction (i.e. 9 gage wire mesh between drywall))
☐ Reinforced ceiling construction (e.g. limits intrusion access through false ceiling)
☐ Motion Sensors
☐ IDS Door Contacts
☐ Other (explain):
☐ Not Applicable
☐ None

**73. Are the System 36/AS400 back-up tapes uniquely labeled to ensure they can quickly be identified?**

☐ Yes
☐ No
☐ Not Applicable

**74. Does the service center backup the information on the System 36/AS400?**

☐ Yes
☐ No

**75. Are the backup tapes for the System 36/AS400 stored in a safe and secure off-site location?**

☐ Yes
☐ No (explain):

**76. Does the location where the backup information is stored meet the protection requirements for PII? (Minimum: Locked filing cabinet)**

☐ Yes
☐ No

**77. Is a key/card log maintained to issue and receive keys/cards for the server room?**

☐ Yes
☐ No

**78. Who signs out/in keys and cards for the server room?**

Name of Key Control Custodian:
Telephone No: (  )  -
E-Mail Address:

**79. Are the server room doors secured at all times?**

☐ Yes
☐ No (explain):

**80. Are the door(s) to the server room either a solid wood core or metal clad door?**

☐ Yes
☐ No

**81. Are there signs on the server room door that identify this area as a server/computer room?**

☐ Yes
☐ No

**82. Is the server room used only for that purpose? If no, please explain.**

☐ Yes
☐ No (explain):

**83. Is the server room free of windows?**

☐ Yes
☐ No

**84. Is the server room cooled at all times, 7 days a week and the ambient room temperature are between 68 to 75 degrees Fahrenheit?**

☐ Yes
☐ No

**85. Are there any temperature or humidity controls located within the server room?**

☐ Yes
☐ No

**86. Are emergency points of contact information posted in the server room?**

☐ Yes
☐ No

**87. Is there a fire extinguisher located in the server space or within 200 feet?**

☐ Yes
☐ No

**88. Are cabinets housing IT equipment locked when unattended?**

☐ Yes
☐ No

**89. Is the server room restricted to mission essential or mission required personnel only?**

☐ Yes
☐ No

**90. Does Janitorial staff have unaccompanied access to the server room?**

☐ Yes
☐ No

**X. <u>Please provide the following attachments:</u>**

- Summary documents of previous security assessments performed at this facility.
- Building floor plan for Service Center (i.e. similar to posted “emergency evacuation floor plan drawing”)
- Summary explanation for any planned capital improvements or plans to modernize the facility and its security.
- Photographs of all exterior entrances, inside server room, front and rear of facility, parking areas and things the site has concerns about.