



USDA

Physical Security Overview

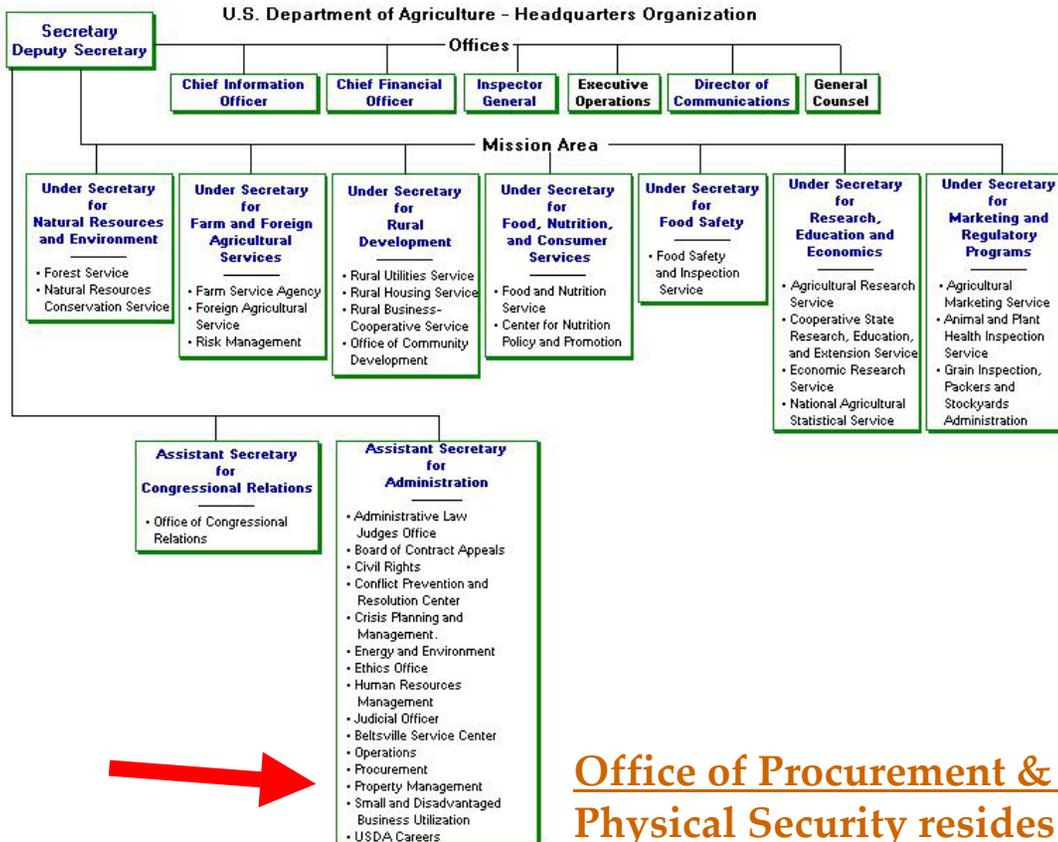


Intent of Briefing

- * Overview of the Physical Security Office
- * Security Assessments w/USDA Agencies
- * Criteria establishing Mission Critical Facilities
- * Methodology used to conduct Security Assessments
- * Physical Security Model
- * On-Going Physical Security Projects



Organization Chart



7 – Mission Areas

27 – Agencies & Offices

97,000+ – Employees

25,000+ - Facilities

Worldwide Presence

Office of Procurement & Property Management (OPPM)
Physical Security resides in the Property Management Division.



Overview of the Property Management Division (USDA)

Personal Property: DA (PMD) manages and coordinates Department-wide personal property, motor vehicle, aircraft, traffic, and acquisition management programs.

USDA owns and accounts for over 675,000 pieces of personal property worth a total acquisition value over \$3.2 billion. The Department owns and operates the fourth largest motor vehicle fleet and the largest civilian aircraft fleet in the Federal Government. DA also manages the Federal Excess Personal Property Program which allows the transfer of excess Federal personal property to eligible recipients as authorized by various authorities; i.e., Federal Agriculture Improvement and Reform Act (Section 923), P.L. 102-245 (Stevenson/Wydler Technology Innovation Act of 1980), and E.O. 12999, Educational Technology: Ensuring Opportunity for All Children in the Next Century.

Real Property: DA (PMD) is responsible for the management of Department-wide real property. As the second largest land holder in the Federal Government, **USDA owns approximately 192 million acres of land (Texas + South Carolina) and occupies approximately 51 million square feet of space (owned and leased) (over 25,000 facilities).** DA assists in management of the central Rent account, through which USDA offices are billed by the General Services Administration (GSA) for their space usage in GSA space.



Agencies Receiving Security Assessments

Natural Resources Conservation Service: Working to assist owners of America's private land with conserving their soil, water, and other natural resources.

Forest Service: Sustain the health, diversity, and productivity of the Nation's forests and grasslands to meet the needs of present and future generations.

Animal & Plant Health Inspection Service: Protecting and promoting U.S. agricultural health, administering the Animal Welfare Act, and carrying out wildlife damage management activities.

Agricultural Research Service: Principal in-house research agency of the Department with 1200 research projects ongoing to protect the nation's food supply.

Foreign Agricultural Service: Works to improve foreign market access for U.S. Products, and bears the primary responsibility for USDA's overseas activities -- market development, international trade agreements and negotiations, and the collection and analysis of statistics and market information.

Food Safety & Inspection Service: FSIS protects the public health by regulating meat, poultry, and egg products, which account for a third of consumer spending for food, with an annual retail value of \$120 billion.

Agricultural Marketing Service: Administers programs that facilitate the efficient, fair marketing of U.S. agricultural Products including food, fibers, and specialty crops.

Rural Development: RD helps rural Americans improve the quality of their lives.



Determining Mission Critical Facilities

Criteria

1	Labs conducting research involving biohazardous materials
2	Labs/Other facilities which must remain operational to protect the nation's food supply
3	Facilities housing valuable germplasm collections which are needed for critical research and testing and cannot be easily replaced
4	Laboratories in foreign countries
5	Departmental computer centers responsible for payroll, program and vendor payments
6	USDA offices in National Capital Region
7	Facilities housing more than 450 employees (by DOJ standards)
8	2002 Winter Olympics
9	Facilities housing headquarters or Field personnel critical to agency mission
10	Alternate Site/COOP Activation
11	BSL-3 labs
12	Mission driven critical research programs



Mission Critical Facilities & Assets Identified

204 Facilities Identified with the following assets to protect

- **97,000+ Personnel** – Throughout the World
- **Aircraft** – Air-tankers WMD, Crop Dusters, etc.
- **Laboratory Equipment** – Diagnostic machines at a cost of up to ½ million dollars each
- **Germplasm** – Used to reconstitute the nations food supply if compromised
- **Location Sites** – Urban, Rural, and sometimes in the middle of no-where
- **Vehicles and Farm Equipment** – Millions of Dollars worth
- **Cattle, Pigs, Deer, Coyote, Sheep, etc.** – Open range & corralled
- **Greenhouse Plants** – Generically Modified Organisms, etc.
- **Biohazardous Materials** – Chemicals, Biological, Radiological
- **Land Management Infrastructure** – Crops, Watershed, SNOTEL (SNOwpack TElemetry), Soil Climate Analysis Network (SCAN) data, etc.



Methodology

- **Asset Identification** - Facility identifies the Asset(s)
- **Criticality Assessment** - Importance of asset to the mission and when the asset is most vulnerable to a threat
- **Threat Assessment** - Used to identify the threat, and its methods of attack from any source or direction
- **Vulnerability Analysis** - Determine the avenues of approach (weakness) to the asset that the threat will take
- **Risk Analysis** - Identify any consequences that may be produced from a compromised asset
- **Gap Analysis** - The difference between existing countermeasures and identified vulnerabilities
- **Security Countermeasure** - A series of security hardware and procedures to counter the identified threat



Asset Identification

Assets – Identified by the facility



Areas of Concern – People, IT infrastructure, Precursors for WMD, Weapons, Chemical materials, Other Items that would be controversial and/or dangerous if released into the public sector, and High Dollar Value Equipment



Asset Identification



Aircraft & Retardant



Data sets (textural/digital) & HDV instruments



Criticality Analysis

Understand mission importance of the asset and when the asset will be most vulnerable to the identified threat/risk. The growing season would be the critical period for GMO research.



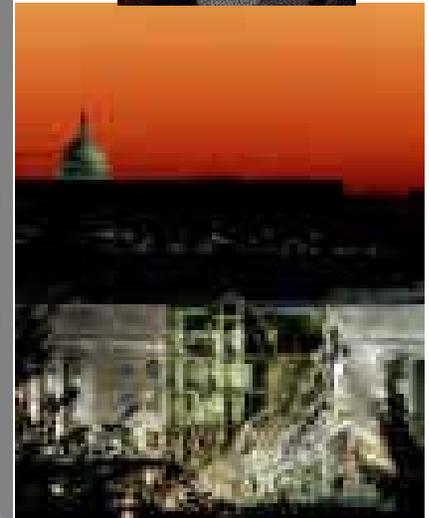
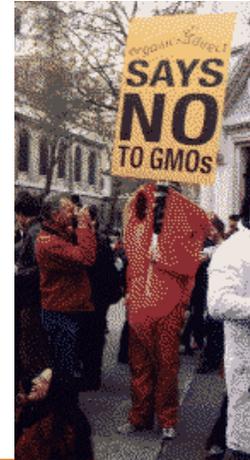


Threat (Credible & Perceived)

Indigenous – These groups mostly are motivated from Individual opposition to USDA in the management of property...forests; research projects...animals, GMO, etc.

Domestic – Opposed to government authority...
Oklahoma bombing

International – Most groups have a political agenda based on an extreme religious belief such as the removal of all Non-Islamic influences from their area.





Threat (Credible & Perceived)

Example: Local Threat - Two mile radius, two year criminal history. FBI, ATF, State, County, City, Site criminal history provides Empirical Data.

Example: Indigenous Threat -

Deleted for Publication



THE THEORY AND PRACTICE OF HELL

"We have enslaved the rest of animal creation and have treated our distant cousins in fur and feathers so badly that beyond doubt, if they were to formulate a religion, they would depict the Devil in human form."

William Ralph Inge



Threat Actions

- * Sabotage/Destruction/Theft
- * Illegal Entry/Trespass (during work hours and after)
- * Suicide Actions/missions
- * Theft of Hazmat
- * Glue Locks
- * Explosive/Fire Bombing
- * Bio/Chemical Attacks...Nuclear?



• Theft of Aircraft (Usually for Drug Operations)

- 340,000 private and student pilots in the country and 18,000 general aviation airports.
- On Sept. 12, 1994, Frank Corder, a truck driver, stole a single-engine plane from a Maryland airport and crashed into the White House



Threat Actions...continued





Threat Probabilities

How likely is it that the asset will be compromised?

Probability of Threat	Threat level description
A. Likely	75% chance that an event will occur during the calendar year
B. Possible	10-74% chance that an event may occur sometime within the calendar year
C. Remote	At least a 1-9% chance an event will occur before the end of the calendar year
D. Improbable	Less than 1% chance an undesired event will occur before the end of the calendar year





Threat Probabilities...continued

Vulnerability Level	Vulnerability description
High	No meaningful physical security measures present (beyond typical locks on doors)
Medium	Some physical security measures; but not adequate to protect against all threats identified in this report
Low	Adequate physical security measures, but could be improved

Event	Event Risk
I. Catastrophic	Death, mission shutdown, severe environmental damage to facility
II. Critical	Severe Injury, partial mission shutdown, some damage to facility environment
III. Marginal	Minor injury, mission time extended, facility affected
IV. Negligible	Less than minor injury, not affecting mission, minor facility damage



Threat Probabilities...continued

Probability of Threat	I. Catastrophic	II. Critical	III. Marginal	IV. Negligible
A. Likely	I A	II A	III A	IV A
B. Possible	I B	II B	III B	IV B
C. Remote	I C	II C	III C	IV C
D. Improbable	I D	II D	III D	IV D

**IA, IIA, IIIA, IB, IIB
IVA, IIIB, IVB, IC
IIC, IIIC, ID
IVC, IID, IIID, IVD**

**Unacceptable (reduce risks through countermeasures)
Undesirable (Management decision required)
Acceptable with review by management
Acceptable without review**



Vulnerability Analysis

Determine the avenues of approach (weakness) to the asset

- Poor Lighting
- No Astragals
- Unlocked Doors
- Unattended Computers
- No Inventories
- No Security Awareness Training
- Uncleared Personnel
- Not safeguarding textural/digital documents properly
- Open access to IT infrastructure





Risk Analysis

Look at the consequences the asset may produce if the vulnerability is not addressed.

Example:

Asset – Twenty-Five 55 gallon drums of chemical waste



Vulnerability - stored on the site's loading dock with no security countermeasures.

Risk - ? (acceptable and unacceptable...which one? What are the possible consequences if compromised?)



Gap Analysis

- Examine the existing security countermeasures that protect the identified asset.
- Understand the severity of the threat (credible or perceived) as it relates to the importance of the asset.
- Based on the importance of the asset, the threat, and the existing countermeasures, make recommendations to construct additional security countermeasures if needed.

Side Note: Seldom if the asset is worth \$10.00 and the threat is low, we will not recommend a \$1,000.00 countermeasure.



Security Countermeasures

C o u n t e r m e a s u r e s

1. Perimeter Fencing w/Gates & top guards
2. CCTV system (Camera, VCR, Multiplexer, Monitor)
3. Intrusion Detection System (IDS)
4. Bollards
5. Positioning of Aircraft
6. Caging Gas Tanks
7. Preflight Check
8. Background Checks
9. Ident-a-kit (badges)
10. Duress Alarms
11. Contract Security Guards
12. Security Awareness/training
13. Generators and/or UPS
14. Testing procedures for Retardant
15. Use of Seals
16. Key-way Locks
17. Lighting (exterior/interior)
18. Security Assessment (Threat, Risk & CM)
19. Barriers
20. Global Positioning (15 min Flight Follow)
21. PROCEDURES...at no cost.





Completion of a Site Assessment

Threat	Stolen aircraft.	 <p>Hanger access key kept outside</p>
Vulnerability	No aircraft hanger security. Although At night the hanger doors are disabled at the breaker box, the breaker box is behind a penetrable door. Several aircraft in position for flight contained aircraft manuals, fuel gauges, cockpit checklists, flight instructor manuals, flight maps, TCMS credit cards all found in aircraft for use by unauthorized pilots	 <p>Hanger doors without locking safety bar</p>
Risks	Through lax hanger security, An aircraft can easily be taken and delivered on target on a sensitive location such as critical infrastructure (Nuclear Power Plants, Dams, etc.)	 <p>Aircraft ready for rollout</p>
Recommendation	1)Initiate immediate physical security enhancements to include re keyed doors, key management system, Updated aircraft hanger procedures, aircraft park procedures, intrusion detection system, hanger door control lock box, CCTV system, universal aircraft anchors, night guard during Olympics. 2)Relocate/disable aircraft during the Olympics	

EXAMPLE ONLY



BV14
 30 min. Range 145 Mi



Completion of Site Assessment

Upon completion of the site assessment, a draft report with countermeasure recommendation will be forwarded to the facility for review and input prior to the final report being sent to the Agency Headquarters.



Follow-Up

After agency review and approval of the security recommendations, a walk through of the site will be scheduled, and then a Systems Integrator will initiate the installation of approved countermeasures at each site

After full installation of security countermeasures, a test will be performed to ensure the installed countermeasures perform to expected security performance levels (Commissioning)

The Systems Integrator will continue to monitor the installed countermeasures and be prepared to assist in any deficiencies

Getting acquainted with the new security procedures and equipment are the most challenging part of the program.



USDA Tiger Team

- Team Leader
- Assessment Coordinator
- Physical Security Specialist
- Information Technology/Telecom Specialist
- Biological/Chemical/Radiological Specialist
- Aircraft Specialist (Pilot)
- Program Manager (Procurement/Acquisitions/Contracts/SOW)
- Production Team...in DC
- Implementation Team (Systems Integrator)



Assembling a Tiger Team

- Use the methodology to guide in the assembly of the team
- Understand the mission and critical functions of the site
- What are the concerns of the site
- Identify skill sets required to conduct the assessment
- Review resumes' of Subject Matter Experts (SME)
- Look at availability of SME...alternates
- Provide Risk Management training to SME
- Observe performance (Performance Base Contract)



Physical Security Model

Example: USDA has an ARS facility in Boise ID that has a CRIS project involving research in GMO (**Asset**). We know by history there is a group of Extremists – (**Threat**) that do not like this type of research. History also shows us that their Modus Operandi is to destroy (burn/slash) the unprotected asset (**Vulnerability**) that would set back research that would cost thousands of dollars and Hundreds of man-hours to recapture the research (**Risk Analysis**). We look at the mission criticality of the asset and the most critical time of risk (**Criticality Assessment**) which is during growing season. Now we look at present protective measures and what is needed (**Gap Analysis**) to protect the asset. We set up our concentric rings of security (**Countermeasures**) starting from the asset working out toward the perimeter. Once the CMs are implemented a **Training** session on each CMs takes place. Now **Test** the CMs and write an **After Action** reports identifying any **Vulnerabilities** in the CMs. Correct the vulnerabilities and test again, until you are satisfied the CMs are adequate to protect against the threat.



On Going Projects

- Physical Security Web Page
- Geographical Security Information System (Database)
- Physical Security Certification Course
- Security Commissioning Process
- Physical Security Policy/Handbook
- Physical Security Self Assessment Tool/Process
- Blue Print and Lease Termination Reviews
- Compliance Reviews (12 facilities per year)



Questions?

