

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY



FOR OFFICIAL USE ONLY

The OIG is issuing this report with the handling instruction "For Official Use Only" (FOUO). The OIG has determined that the report contains sensitive information that should not be released to the general public. Recipients of this report must protect it from unauthorized disclosure and should not make further dissemination of the report.

OIG-07-43

May 2007

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

May 21, 2007

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report summarizes our assessment of the adequacy and effectiveness of the physical and system security controls implemented at Plum Island Animal Disease Center (PIADC). It includes an evaluation of PIADC's compliance with the Federal Information Security Management Act (FISMA) requirements, including the physical security findings previously reported by the Government Accountability Office (GAO) in September 2003. It is based on interviews with employees and officials of relevant federal and local agencies, direct observations and analyses, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background	2
Results of Audit	5
Physical Security Measures	5
Physical Security Measures Implemented	6
GAO Reported Issues Addressed	8
Physical Security Concerns	9
Operations and Maintenance Contract Administration Issues	13
Need of a Continuity of Operations Plan	13
Recommendations	14
Management Comments and OIG Analysis	15
System Security Controls	17
System Security Vulnerabilities Identified	17
PIADC Network Implementation Concerns	20
Results of Wireless Security Scans	21
Improved IT Security Program and Structure Needed	22
Recommendations	24
Management Comments and OIG Analysis	24
FISMA Compliance	25
Recommendations	27
Management Comments and OIG Analysis	28

Appendices

Appendix A: Purpose, Scope, and Methodology	30
Appendix B: Management's Response	34
Appendix C: Summary of Significant Security Vulnerabilities Identified and Potential Threats	40
Appendix D: Major Contributors to This Report	45
Appendix E: Report Distribution	46

FOR OFFICIAL USE ONLY

Table of Contents/Abbreviations

Abbreviations

AC	Apple Cluster
C&A	Certification and Accreditation
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CSA	Comprehensive Security Assessment
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IAVM	Information Assurance Vulnerability Management
ISA	Interconnection Security Agreement
ISS	Internet Security Systems
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
MAC	Macintosh
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
O&M	Operations and Maintenance
OS	Operating System
PIADC	Plum Island Animal Disease Center
POA&M	Plan of Action and Milestones
[REDACTED]	[REDACTED]
S&T	Science and Technology
TCS	Tactical Communications System
USDA	U.S. Department of Agriculture

b2 per
S&T

Additional Physical, System, and Management Controls Can Enhance Security At Plum Island

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the effectiveness of physical security and logical access controls over Department of Homeland Security systems and data housed at the Plum Island Animal Disease Center. The Plum Island Animal Disease Center is a unique scientific animal research facility and a critical national asset, located on Plum Island, New York. The Department of Homeland Security, under its Science and Technology Directorate, assumed responsibility for the administration and management, including facility security, of the Plum Island Animal Disease Center from the U.S. Department of Agriculture in June 2003. The department later assumed responsibility for systems security in October 2006.

Our audit work focused on an on-site evaluation of the physical security measures and policies implemented for Plum Island, and the access controls over the Department of Homeland Security's systems located at Plum Island Animal Disease Center. It also included an evaluation of the department's compliance with the Federal Information Security Management Act requirements and physical security concerns reported by the Government Accountability Office in September 2003. Fieldwork was conducted between October and December 2006.

Under Department of Homeland Security leadership, effective physical security measures have been implemented at the Plum Island Animal Disease Center. All but one of the Government Accountability Office's physical security recommendations have been addressed. The system security issues identified, however, weaken Plum Island's information technology security program and should be addressed prior to implementation of the planned Plum Island network. Additionally, compliance with Federal Information Security Management Act requirements, government information technology standards, and industry best practices are

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

important factors in providing security for the information and the information systems that support the Plum Island Animal Disease Center's operations and assets.

We are making six recommendations to further enhance Plum Island's physical and logical access security measures. Plum Island's physical and system security controls are integral elements in effectively implementing an information technology security program at Plum Island. Our physical security recommendations focus on improving the controls implemented for protecting against unauthorized access to and disclosure of Plum Island Animal Disease Center's sensitive systems and data. The four additional system security recommendations are aimed at improving Plum Island Animal Disease Center's compliance with Department of Homeland Security information technology security policies and procedures.

In response to our draft report, S&T concurred with our recommendations. S&T's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

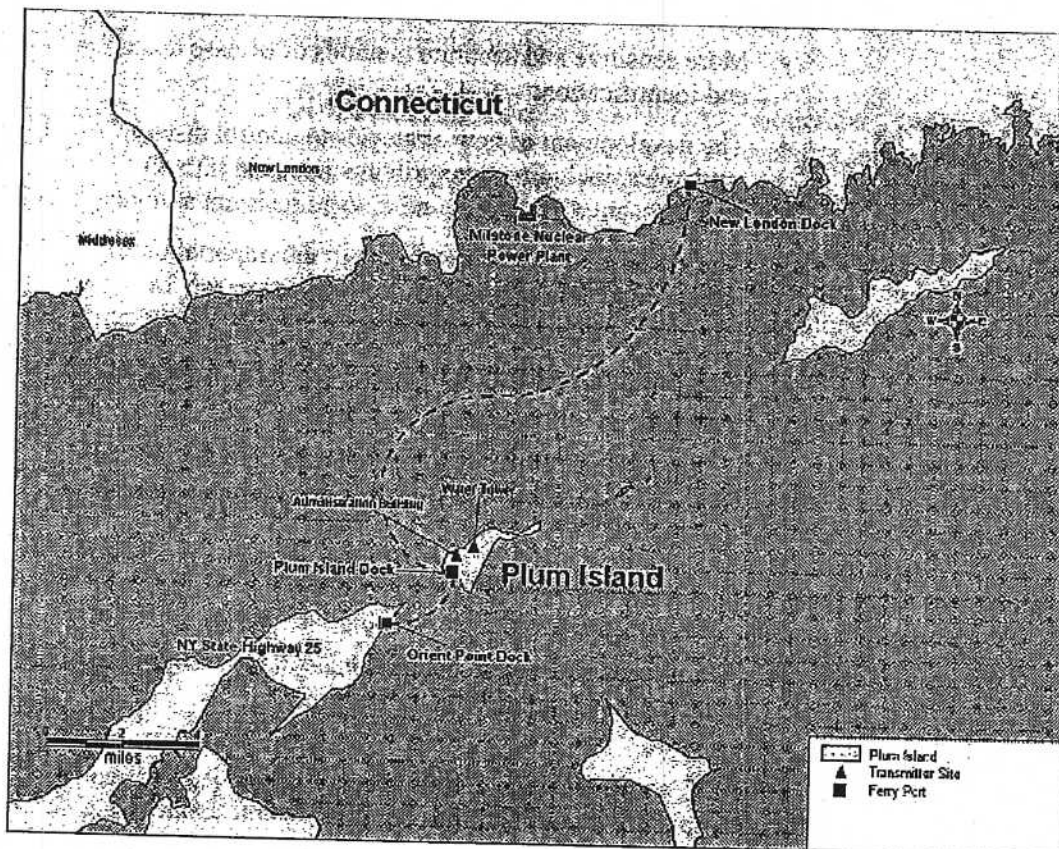
Background

Plum Island is a federally owned 840-acre island off the tip of Long Island, New York, and home to the Plum Island Animal Disease Center (PIADC). Formerly operated solely by the U.S. Department of Agriculture (USDA), PIADC became part of the Department of Homeland Security (DHS), as mandated by the Homeland Security Act of 2002, on June 1, 2003 (PL 107-296, Section 310). Access to Plum Island is by DHS-owned ferry service, operated by a DHS contractor, that transports employees and authorized visitors from Orient Point, New York, and Old Saybrook, Connecticut (see Figure 1).

Currently, PIADC conducts research on foreign animal diseases that are not present in the United States, with a primary focus on foot-and-mouth disease. PIADC also studies infectious diseases of cattle, swine, goats, and poultry. PIADC's contribution to animal

disease research dates back to 1951, under auspices of the U.S. Army Chemical Corps. In the 1940s and 1950s, the U.S. Congress appropriated funds for a new laboratory in response to outbreaks of foot-and-mouth disease in Mexico (1946) and Canada (1952). The new facilities constructed were then transferred to USDA.

Figure 1: Plum Island Geographic Map



FOR OFFICIAL USE ONLY

PIADC's mission is to develop strategies for protecting the Nation's animal industries and exports from foreign animal diseases, which could be accidentally or deliberately released in the United States. International scientific collaboration and commercialization of vaccines and diagnostic tools remain salient features of PIADC's research agenda. The PIADC mission is accomplished by:

- More sensitive and accurate methods of disease detection and identification;
- The development of new strategies to control disease epidemics, including deoxyribonucleic acid (DNA) vaccines, antiviral drugs, and disease-resistant animals;
- The assessment of risks involved in the importation of animals and animal products from countries where epidemic, foreign animal diseases occur;
- Diagnostic investigation of suspect cases of foreign animal disease;
- Testing animal products to be imported into the United States to ensure they are free of foreign animal disease agents;
- Production and maintenance of reagents used in diagnostic tests and vaccines; and
- Training animal health professionals in the recognition and diagnosis of foreign animal diseases.

The PIADC's island setting and its specially designed and sealed biocontainment area and facilities permit safe and secure research. While USDA personnel continue their research, development, and diagnostics programs at PIADC, DHS personnel have assumed the administrative and management responsibilities, encompassing utilities; transportation; facilities and grounds; biocontainment needs; facility security; fire protection and emergency medical services; environmental management; warehousing; operations; and maintenance.

FOR OFFICIAL USE ONLY

DHS has a mission to protect the United States from terrorist threats, including those directed against agriculture. Some of the biological agents and toxins maintained at PIADC, such as the foot-and-mouth disease virus, are highly contagious to livestock and can cause illness and death in animals. The transfer of PIADC operations to DHS facilitates the department's ability to lead a focused research and development program to prevent, respond to, and recover from the intentional introduction of diseases to the general animal population.

DHS is working closely with USDA to modernize PIADC's facilities to support their joint agro-terrorism mission. The department has implemented a corrective action plan to address needed facility and systems upgrades to improve the overall security at PIADC. These upgrades include additional physical security measures, as well as the creation of the Plum Island network, which will connect PIADC's standalone systems on one network.

PIADC's physical security measures serve as mitigating controls for protecting access to the island, facilities, systems, and data, while the system security controls reduce the risks associated with the loss, misuse, and access to or modification of sensitive data. It is imperative that PIADC implement robust security measures to protect the research conducted from the catastrophic consequences that could result from the accidental or deliberate introduction of foreign animal disease agents into the U.S. animal industries, food supply, and exports.

Results of Audit

Physical Security Measures

Our on-site assessment of physical security at PIADC included an evaluation of the physical security controls implemented for the ferry service; island grounds and surrounding environment; main building, including the security control center and computer server room; and biocontainment areas. PIADC's main building, Building [REDACTED] houses the facility's administrative offices,

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

Page 5

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

b2, 7F
per S&T

conference rooms, security control center, and computer server room. [REDACTED]

Generally, physical security controls at PIADC are adequate. Still, there are a number of enhancements PIADC can take to strengthen security at this critical site.

Physical Security Measures Implemented

Overall, PIADC has implemented adequate facility physical security measures. The controls put into practice are operating effectively to safeguard personnel and reduce the risk of unauthorized access to, and the loss, theft, destruction, sabotage, or compromise of equipment, material, and sensitive information. For example, PIADC has:

- Developed a comprehensive security plan that established the parameters for the physical, informational, and organizational bio-security and safety measures in operation;
- Implemented policies and procedures for granting and authenticating facility access to employees, visitors, and contractors, including a code of conduct for employees and visitors, as well as other personnel security measures;
- Established standard operating procedures for most emergency situations, which include plans for adverse weather, bomb threats, spills, power outages, and exiting biocontainment without personal biological decontamination - these plans include "check-off" sheets that are to be completed when the plans are tested and when an event occurs to ensure the situation is documented and that the proper procedures were followed;
- Installed security cameras, including infrared cameras, within its administrative and biocontainment buildings, outside of critical facilities, such as the power and water supplies, and surrounding the island's perimeter; and
- Implemented requirements for entry security, including shipping and receiving, parking, electronic surveillance, and alarm systems.

Exhibit 1 illustrates examples of physical security measures employed at PIADC.

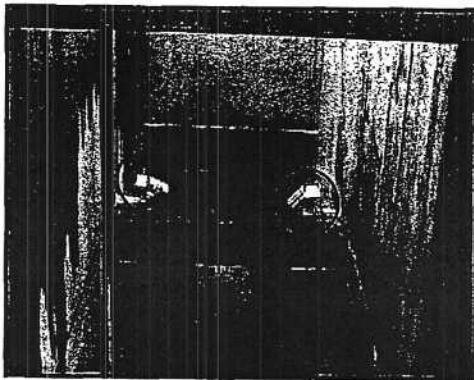
Exhibit 1: Examples of Physical Security Measures Employed



Signs Surrounding Building



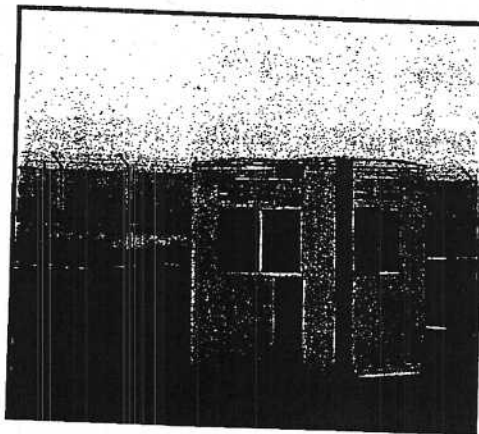
Building Gate Sign



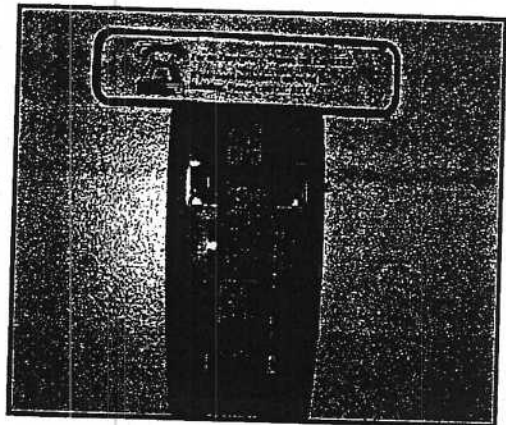
Secured Access Door Outside of Biocontainment

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island



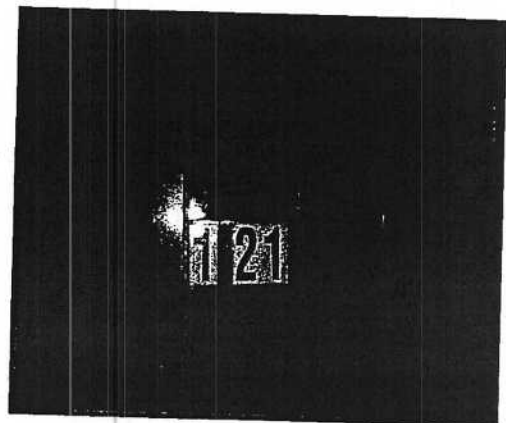
Manned Outside Security Post



Security Emergency Numbers Posted On All Phones



Manned Checkpoint Prior to Biocontainment Entrance



Indoor Entrance to Biocontainment Area

Government Accountability Office (GAO) Reported Issues Addressed

In September 2003, GAO recommended specific actions to improve physical security at PIADC.¹ We followed up on the actions taken to address GAO's concerns and determined that PIADC:

¹ *Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center*, GAO-03-847, September 2003.

- Implemented policies and procedures for intruder response; guards' authority to carry firearms; emergency situations; and background checks for employees, visitors, and contractors;
- Developed strict rules to control access to the biocontainment area;
- Implemented island security patrols that operate 24 hours a day/7 days a week;
- Created a keycard database and key log to track the possession of keycards; and
- Posted "No Trespassing" signs around the island to better deter unauthorized visitors.

GAO also reported that PIADC needed to improve on aspects of perimeter security, including lighting, and continuity of operations planning. These issues remain concerns and are discussed further in other sections of this report.

Physical Security Concerns

Due to the mission and the scientific work conducted, PIADC and all properties associated with PIADC, to include the Orient Point, New York, parking facility, are considered "restricted access" areas. According to PIADC's Visiting Program policy, the general public is not authorized to enter onto PIADC's premises. Individuals must have a purpose or official business that is relevant to PIADC's mission to be permitted to visit the island. Therefore, the physical security measures and procedures implemented are important in deterring unauthorized persons from attempting to gain access to all locations. While PIADC has implemented numerous physical security measures, some physical access concerns remain as follows.

Search Procedures

According to PIADC's visiting program and post orders, security guards are to obtain identification and search personal property, belongings, and carry-on materials brought on by visitors prior to boarding the ferry to or departing from PIADC. Though procedures and post orders have been implemented for visitors and

FOR OFFICIAL USE ONLY

employees arriving and departing Plum Island, neither specifically stresses or details the process for comprehensive, consistent searches of visitors and their property.

During our visit to PIADC, we observed that the search procedures for visitors arriving and departing the island were not consistent. For example, we noted that on some nights, guards used flashlights to search bags, while on other nights flashlights were not used. The guards did not always check women's purses, winter coats, or pockets. Visitors were not always questioned about restricted items, which include video, photo, or digital cameras; food; and liquids.

PIADC's standards and procedures for visitors were established to safeguard the public, the biological agents, PIADC employees, and the facilities from threats of danger, unauthorized access, damage, and theft. However, since PIADC's search process is neither comprehensive nor consistent, there is little assurance that visitors are complying, which may increase security risks associated with authorized or unauthorized access to the facility.

Server Room Security

Security control center guards monitor the computer server entrance door via closed circuit television. Employees access the server room using their keycards. For visitors, however, there is no logbook to record who enters and exits the computer server room. Additionally, we observed maintenance contractors working inside the room who were not escorted or monitored.

Based on the criticality of the systems and the sensitivity of the data being processed, information technology (IT) systems must be physically and environmentally protected to prevent unauthorized disclosure, denial of service, destruction, and modification. DHS policy requires that controls be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. All visitors are to be escorted and sign in and out upon entering and leaving a facility, including rooms containing IT equipment. Keeping a logbook, ensuring that uncleared contractor personnel are escorted, and requiring that all contractors be monitored at all times are best practices.

FOR OFFICIAL USE ONLY

Perimeter Security

Although PIADC implemented a number of best practices for perimeter security and electronic surveillance, we observed the following:

- [REDACTED] Also, in certain areas such as the ferry docks, the [REDACTED]

GAO also reported a concern with the lighting on the island.

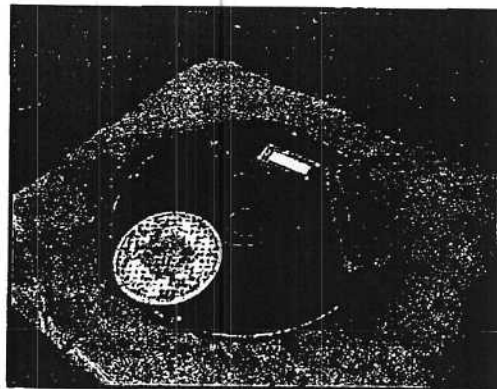
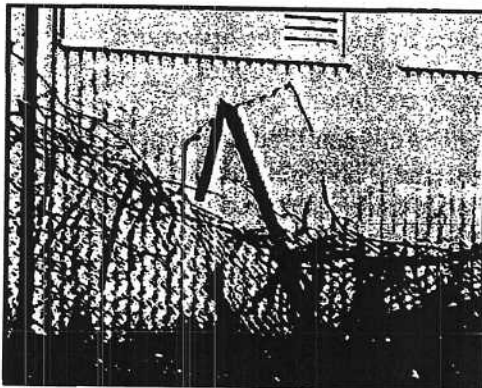
- [REDACTED]
- There is damage to the security fence surrounding Buildings [REDACTED]

- [REDACTED]

b2, 7F
per S&T

Exhibit 2 illustrates our last two concerns.

Exhibit 2: Examples of Physical Security Concerns



Manhole Cover to Underground [REDACTED]

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

b2, 7F
per S&T

[REDACTED] Also, according to industry best practices, [REDACTED] should be protected from intruders with [REDACTED]; there should be no damage or deterioration to physical barriers at perimeter lines; [REDACTED]

We discussed the physical security concerns with Science and Technology (S&T) management. S&T management said that, upon assuming responsibility for PIADC in June 2003, DHS conducted an internal assessment and commissioned an external review to create a list of needed facility and systems upgrades, which also incorporated the results of the 2003 GAO audit. In December 2004, DHS developed a corrective action plan to address needed facility and systems upgrades to improve the overall security at PIADC. At that time, the major upgrades identified in the plan were estimated to be \$56.1 million as of December 2006.

Specifically, the plan concentrated on the safety of the workers, security of the facility, and protection of the environment through planned upgrades for PIADC's security program and alarm systems; IT and communications systems; buildings, grounds, and infrastructure systems; environmental, health, and safety systems; and administration and management program. The plan demonstrates S&T's commitment to improve the operations, maintenance, safety, and security at PIADC facilities.

S&T took some immediate actions on identified deficiencies that could be corrected through procedural changes and did not require funding. Other, planned upgrades were prioritized for funding based on the need to meet safety and security requirements, remain in compliance with federal or state requirements, and deliver the broadest impact to dollars expended.

FOR OFFICIAL USE ONLY

Operations and Maintenance (O&M) Contract Administration Issues

S&T contracts out O&M support services, including facility and equipment repairs, at PIADC.² As such, the contractor is responsible for performing operations and maintenance, ensuring site safety and security, and providing other facility, environmental management, and support services in accordance with the performance work statement and the terms and conditions of the contract. The quality assurance specialist is responsible for monitoring, assessing, recording, and reporting on the technical performance of the contractor on a continuous, day-to-day basis.

We determined, however, that the contract requirements are not being monitored, and there is increased risk that certain performance requirements are not being met. For example, the fire alarm monitoring minimum standards of performance require that the contractor provide a weekly fire system log and test the fire alarms monthly. We discovered that the contractor has not provided either the weekly fire system log or tested the fire alarm monthly as required by the contract. PIADC personnel were not aware of this requirement. S&T agreed that there were deficiencies with the language and management of the contract, as well as problems with funding, definition of "functional responsibilities," and the execution of the contract.

Need of a Continuity of Operations Plan (COOP)

PIADC has implemented a number of plans to deal with different physical security contingencies, such as intruder response; adverse and severe weather; suspicious packages; power outages; access to the vaccine bank; disaster recovery; fire response; and biosafety/biosecurity. Maintaining the continuity of business operations and services to support the research and diagnostic

² The following are included under the O&M contract: laboratory and animal-handling facilities (Building █ main administrative personnel building (Building █ grounds; motor pool; duty officer's quarters; fire house; shop building; and support facilities, such as the waste water treatment plant, utilities buildings; electrical and telecommunications distribution systems; chiller plant, construction of the power facility; and transporting employees and visitors to PIADC (i.e., ferry).

b2, 7F
per S&T

FOR OFFICIAL USE ONLY

activities conducted should also be a priority. However, PIADC has not implemented a COOP in order to ensure that its essential functions continue in the event an emergency prevents occupancy of its primary facility. A COOP provides an organization with an operational framework for continuing its essential functions when normal operations are disrupted or otherwise cannot be conducted from its primary facility. A draft COOP has been developed, but DHS has neither reviewed nor approved the plan.

DHS requires that an organization ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies. The efforts agreed upon should then be documented through plans and procedures that:

- Delineate essential functions and supporting IT systems;
- Provide for the safekeeping of vital records and databases;
- Identify alternate operating facilities;
- Provide for interoperable communications; and
- Validate the capability through tests, training, and exercises.

Recommendations

We recommend that the Under Secretary, S&T, instruct its Director of Security to:

1. Document specific procedures and provide training for PIADC security guards to ensure comprehensive and consistent searches of people and their properties are occurring when arriving and departing Plum Island.
2. Implement a server room policy requiring visitors to sign in, notate the date and time, and sign out of the room, and ensure that uncleared contractor personnel are escorted to the server room and monitored at all times.
3. Enhance the physical security measures implemented around the island's perimeter, facility buildings, and supporting infrastructure to include [REDACTED]

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

4. Revise the draft COOP based on the results of an updated risk assessment and contingencies. The Director of Security should also temporarily implement the draft plan to ensure continued facility operations in the case of an unexpected catastrophic event.

We recommend that the Under Secretary, S&T, direct the Lab Operations Team Lead to:

5. Update the corrective action plan to incorporate physical security improvements regarding the search process, server room security, perimeter security measures, and electronic surveillance, as well as continuing to reflect current cost estimates.
6. Improve the oversight of the performance and quality of services being provided under the O&M contract by providing contracting officials with additional training and amending the contract if necessary.

Management Comments and OIG Analysis

S&T concurred with recommendation 1. A review is being conducted of the Security Guard Post Orders that describe search requirements of personnel, packages, and vehicles entering and exiting Plum Island. Appropriate changes will be made to reflect consistency in search requirements and training for the guard force will be conducted.

We accept S&T's response to address the Security Guard Post Orders and to provide training for the guard force to ensure comprehensive and consistent searches of people, their property, and vehicles entering and exiting Plum Island.

S&T concurred with recommendation 2. In accordance with the Plum Island Security Plan, uncleared personnel are not permitted unescorted access to the server room. All uncleared personnel are monitored at all times while in the server room. Security and IT will implement a visitor sign-in log.

FOR OFFICIAL USE ONLY

We accept S&T's response to ensure that uncleared personnel are escorted to the server room and monitored at all times, and to implement a visitor sign-in log.

S&T concurred with recommendation 3. S&T has developed a statement of work with the assistance of the Army Corps of Engineers, Electronic Security Center, Huntsville, Alabama, that captures the comprehensive physical security enhancements that will correct the deficiencies detailed in the OIG report. The services of an architect/engineering firm are in the process of being solicited to develop the construction detail for soliciting bids on the work. A schedule for the completion of each phase is being developed.

We accept S&T's response to work with the Army Corps of Engineers' Electronic Security Center to address physical security deficiencies.

S&T concurred with recommendation 4. The update and revision of the COOP is an ongoing process. All pertinent risk assessment data will be considered in developing the final plan and its revisions. Separate from the COOP, there are emergency operation and disaster recovery plans in place to deal with emergencies and unexpected events.

We accept S&T's response to consider pertinent risk assessment data when developing the final COOP. We acknowledge that PIADC has implemented emergency operation and disaster recovery plans. Nonetheless, we place emphasis on the need to approve and implement the final COOP to ensure the continuity of business operations and services to support PIADC's research and diagnostic activities in the event an emergency may prevent the occupancy of its primary facility.

S&T concurred with recommendation 5. The statement of work referred to in recommendation 3 will address all known security issues. The CAP, as reported to Congress, is refined and updated as new information becomes available and/or as tasks are

implemented for completion. The statement of work with detailed costs and a completion schedule is being developed. DHS is utilizing a variety of in-house and contractor specialists to address each of the areas and plan the execution of the detailed projects.

We accept S&T's response in regard to updating the CAP.

S&T concurred with recommendation 6. S&T now has an on-site contracting officer devoted to the oversight of the O&M contractor to improve performance and quality of service. In addition, the contract will be up for re-bid in two years and the contracting officer will address any significant changes required.

We accept S&T's response to improve the oversight of the O&M contractor and address any significant changes when the contract is up for re-bid.

System Security Controls

PIADC's system security controls are adequate to protect the sensitive data contained within them in their current environment. This is in part due to the physical security measures in place and the fact that these are standalone systems. System security vulnerabilities exist that should be addressed before the current configuration is changed, particularly in the construction of the proposed Plum Island network.

System Security Vulnerabilities Identified

Seven PIADC systems were transferred from USDA to S&T as of October 1, 2006. Four of the seven systems transferred to S&T were operational; three were in development. The scope of our audit did not include the systems in development.

The following systems are operational:

- **Apple Cluster (AC)** – AC is used to process DNA sequences that are downloaded from a public website, through an Internet connection on the USDA's Agricultural Research Service network. PIADC scientists and researchers use the AC to carry

FOR OFFICIAL USE ONLY

out DNA evaluations and transmit the results and other research information.

- **Security System** – PIADC's Security System provides electronic entry control, intrusion detection, and closed circuit television surveillance and assessment. The system combines all physical access controls, alarms and surveillance components into a seamless monitoring and control system.
- **Siemens System** – Siemens System is used to control the heating, ventilation, and air conditioning in the lab areas. Siemens technicians and contractors manage the system.
- **Tactical Communications System (TCS)** – TCS is a [REDACTED] designed to provide land mobile radio communications capabilities among PIADC's security force. [REDACTED]

b2, 7F
per S&T

In addition, PIADC has connections to DHS' A-LAN. Plum Island's DHS employees connect to the A-LAN to exchange email and access the Internet. The A-LAN is the only DHS network connection for PIADC's DHS employees. The Infrastructure Security Division, DHS Headquarters, remotely manages the A-LAN connection on Plum Island. S&T is not responsible for managing Plum Island's A-LAN connection.

We detected more than 500 instances of security vulnerabilities during the security vulnerability assessments of PIADC's DHS-owned systems. The total number of instances includes the number of vulnerabilities detected from our scans of the AC, Security System, Siemens System, TCS, and A-LAN. These system vulnerabilities identified can leave PIADC vulnerable to various internal and external security threats that can adversely affect its mission.

Specifically, of the 539 security vulnerabilities identified, 93 were classified as "high" risk, and 236 were classified as "medium" risk. The remaining 210 vulnerabilities identified were classified as "low" risk. Figure 2 documents the number of high, medium, and

FOR OFFICIAL USE ONLY

low vulnerabilities detected by system. The tools used to conduct our scans are described in detail in Appendix A.

Figure 2: Instances of Security Vulnerabilities Detected by System

Systems		Medium		Total
AC	36	3	172	211
Security System	9	7	22	38
Siemens System	42	137	12	191
TCS	6	88	2	96
A-LAN	0	1	2	3
Totals	93	236	210	539

The majority of high-risk vulnerabilities were related to patch management and configuration settings. Other vulnerabilities were related to identification and authorization, application security, and system integrity (system integrity involves audit logging and backup requirements). Appendix D contains a summary of the significant (i.e., high risk) vulnerabilities and the potential system security threats. Specific examples of vulnerabilities detected include:

b2, 7F
per S&T

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

b2, 7F
per S&T

[REDACTED]

The existing vulnerabilities may allow malicious or careless users to compromise the confidentiality, integrity, and availability of sensitive PIADC research data; disrupt the electronic entry control, intrusion detection, and closed circuit television surveillance systems; affect the heating, ventilation, and air conditioning in the lab areas; and interrupt the radio communications capabilities among PIADC's security force. PIADC's sensitive research data can be lost, corrupted, or compromised through the acts of malicious or careless users. Email can be used, either deliberately or unintentionally, to transmit sensitive data outside the department to recipients or other computer systems that are not authorized to receive or store the data. Departmental computers can also be used to attack other computers within and outside of DHS.

PIADC Network Implementation Concerns

The risk of malicious system security attacks are minimized because PIADC's systems are isolated on the island, there are few users assigned access, and each of the four operational systems assessed are disparate, standalone systems. Additionally, the physical access controls implemented reduce the risks associated with the systems.

Nevertheless, the vulnerabilities identified need to be addressed prior to S&T's implementation of the planned Plum Island network, which will connect PIADC's systems on a single network. The high-risk system security vulnerabilities detected pose significantly greater risks in developing, certifying, and accrediting a network environment and could impact the realization and timeliness of the Plum Island network.

Another factor impacting the implementation of the Plum Island network is related to the physical infrastructure of the computer server room. PIADC is undergoing a server room re-wiring project that has yet to be completed to establish an A-LAN connection for approximately 70 DHS users' computers. These

FOR OFFICIAL USE ONLY

computers were assigned to former USDA employees who had migrated to DHS. We discovered that these 70 computers were still connected to USDA's network because the re-wiring has been an ongoing project. S&T has no control over USDA's network. DHS policy requires that system owners understand and appropriately address risks, especially interconnectivity with other systems outside their control, which, in this case, would be USDA's network.

We discussed the system security vulnerabilities detected and the potential impact on the implementation of the Plum Island network if they were not addressed by S&T's IT management. S&T agreed that there were significant IT system concerns and agreed to work on the system weaknesses in order to reduce the security threats prior to implementing the planned Plum Island network. Prior to the end of fieldwork, S&T had updated its Plans of Action and Milestones (POA&M) to address the system vulnerabilities we detected.³

Results of Wireless Security Scans

b2, 7F
per S&T

Wireless systems are vulnerable to a number of traditional attacks and attacks specific to wireless technologies. These attacks fall into the following categories: unauthorized access, denial-of-service/jamming/interference, signal detection, masquerading, and message modification. We conducted wireless security scans both within and outside of Building [REDACTED] to determine the presence of any rogue access points, devices, or networks that may be susceptible to intrusion by unauthorized personnel or may pose any security threat to PIADC's operations.

Overall, we did not detect any authorized or unauthorized wireless devices on DHS systems or rogue access points on the island. We did, however, detect multiple wireless devices connected to USDA's network. These devices could impact the security of the DHS network since 70 DHS workstations are still connected to USDA's network. Additionally, because of the sensitive research conducted on the island, PIADC is also susceptible to foreign threats, and wireless communications are vulnerable to

³ The POA&M serves as a management tool for addressing and resolving security-related weaknesses.

eavesdropping. To comply with DHS' IT security policy, specific countermeasures may need to be implemented based on USDA's decision to allow or ban wireless devices.

Improved IT Security Program and Structure Needed

In order to ensure the security of DHS' IT resources, basic security management principles must be followed. DHS' IT security policies delineate the security management structure and lay the foundation necessary to measure progress and compliance. As currently established, PIADC's IT structure does not allow for a robust system security program to properly and effectively manage security risks and ensure compliance with DHS policy.

For example, an Information Systems Security Officer (ISSO) has not been appointed to oversee and administer PIADC's IT security program. According to DHS policy, an ISSO should be designated for every DHS IT system. An ISSO is to serve as the principal point of contact for all IT security aspects pertaining to the IT systems for which the ISSO is responsible, including working closely with the Information Systems Security Manager and other DHS Chief Information Security Office staff, as appropriate, to interpret and apply IT security policies and implement procedures.

Currently, PIADC is depending heavily on an interim ISSO, who is located at S&T Headquarters, not on site, to ensure that PIADC's systems are secure, in compliance with DHS policies, and system security concerns, issues, and deficiencies are properly addressed. There is also little communication and coordination regarding system security issues between DHS and USDA personnel. As a result, PIADC management did not have an overall awareness of the current security posture of PIADC's IT program and system vulnerabilities that exist. Furthermore, in our opinion, some of the IT security program issues identified exist because a permanent center director has not been appointed to manage PIADC. A permanent center director would provide the leadership, decision-making authority, and ownership of the system security program locally.

FOR OFFICIAL USE ONLY

In addition to the issues with PIADC's IT security program structure, the following were identified concerning the administration of PIADC's systems:

- PIADC system personnel had not implemented rules of behavior or followed a separation of duties policy.⁴
- PIADC's systems were not installed in compliance with DHS' system configuration standards.
- [REDACTED]
- System performance was not monitored.
- Procedures to ensure software changes were authorized, documented, implemented, and maintained, were not implemented.
- System and network diagrams to represent the configuration baselines of PIADC's systems did not exist.
- [REDACTED]

b2, 7F
per S&T

PIADC needs to improve its system administration in order to reduce these threats and comply with DHS policy. The proper administration of systems and the implementation of security controls and policies help ensure the confidentiality, integrity, and availability of sensitive information. A separation of duties is necessary to maintain adequate internal control of sensitive IT systems; ensure that no single individual has total control of the system's security mechanisms; and, prevent a single individual alone from subverting a critical process or otherwise compromise systems.

⁴ Rules of behavior inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS systems and using DHS IT resources capable of accessing, storing, receiving, or transmitting sensitive information. A separation of duties mandates the assignment of portions of security-related tasks to several individuals, ensuring that no single individual has total control of the system's security mechanisms.

Recommendations

We recommend that the Under Secretary, S&T, direct its Acting CIO to:

7. Address system security vulnerabilities identified prior to implementation of the Plum Island network;
8. Train current PIADC system personnel to implement and follow DHS' system administration policies and procedures;
9. Appoint a permanent, on-site ISSO at PIADC to ensure DHS security policies are applied and oversee the implementation of DHS procedures; and
10. Hire a center director to provide direction and focus on PIADC's IT security program and management.

Management Comments and OIG Analysis

S&T concurred with recommendation 7. S&T has planned for the interim ISSO to go to PIADC for one week to begin the process of addressing the system vulnerabilities. All systems will be evaluated and the vulnerabilities will be mitigated. This will be completed before the implementation of the Plum Island network.

We accept S&T's response to address system security vulnerabilities identified prior to the implementation of the Plum Island network.

S&T concurred with recommendation 8. Currently, PIADC management is interviewing for a full time ISSO. The ISSO will be responsible for training all PIADC system personnel and implement DHS system administration policies and oversee the implementation of DHS system administration procedures.

We accept S&T's response to hire a full time ISSO whose responsibilities would include training all PIADC system personnel and implementing DHS' system administration policies and procedures.

FOR OFFICIAL USE ONLY

S&T concurred with recommendation 9. As previously stated, PIADC management is interviewing for a full time ISSO. The ISSO will be responsible for ensuring all DHS security policies are applied and also oversee the implementation of DHS sensitive system security procedures.

We accept S&T's response to hire a full time ISSO whose responsibilities would include ensuring that all DHS security policies are applied and also overseeing the implementation of DHS sensitive system security procedures.

S&T concurred with recommendation 10. Management is currently looking to fill the center director position.

We accept S&T's response to hire a center director.

FISMA Compliance

Based on our analysis of the security documentation for PIADC's systems, we determined that the interim ISSO has made progress in ensuring that the systems transferred from USDA to S&T are in compliance with DHS' FISMA requirements. Current efforts are underway to address the following deficiencies identified as they directly relate to FISMA.

System Certification and Accreditation (C&A)

All DHS systems (major applications, general support systems) are to undergo C&A. Three of the four operational systems transferred to S&T have not been certified or accredited. S&T is taking steps towards the C&A of the other three systems, but much of the required supporting documentation is in draft or does not exist.

DHS policy requires all systems to be certified and accredited prior to becoming operational. Certification is the comprehensive testing and evaluation of the management, operational, and technical IT security features and of other safeguards of an IT system. Certification primarily addresses software and hardware security safeguards, but it also considers procedural, physical, and personnel security measures employed to enforce IT security policy. Accreditation covers the activities leading to the

authorization of an IT system to process, store, and transmit information.

IT Contingency Planning

PIADC has drafted IT contingency plans for three of its four operational systems, but none of these plans have been approved or implemented. For the remaining system, a contingency plan has been implemented, but the testing results were not documented.

Contingency planning should ensure the continuous availability of critical IT systems, protect IT assets and vital records, mitigate disruptions to operations, provide maximum safety to personnel, minimize damage to assets, and achieve a timely and orderly recovery from a disruption to operations. DHS components are required to develop, test, and maintain IT contingency plans to ensure adequate IT services are available to sustain the department's essential and supporting office functions.

At a minimum, IT contingency plans shall be tested annually. Testing identifies planning gaps and serves to validate specific aspects of contingency plans, policies, procedures, systems, and facilities to be used during an emergency. Both activities improve plan effectiveness and overall agency preparedness.

Memorandums of Understanding (MOU)/Interconnection Security Agreements (ISA)

Neither an MOU nor an ISA were established between DHS and USDA to govern the connection of the systems owned by these organizations at PIADC. Though approximately 70 DHS systems are connected to USDA's network, S&T had little knowledge regarding the IT security posture of USDA's network, including whether the network had been certified and accredited. An MOU and an ISA should have been developed between DHS and USDA prior to connecting the systems to ensure that the connection is secure and that neither DHS nor PIADC data can be compromised.

MOUs and ISAs are vital in protecting the confidentiality, integrity, and availability of the data processed between interconnected IT systems. ISAs formalize the security

FOR OFFICIAL USE ONLY

understanding between the authorities responsible for the electronic connection between systems, including an assurance that the interconnected systems are certified and accredited prior to establishing a connection.

Organizations that own and operate IT systems that will be connected are required to document the technical requirements of the interconnection in an ISA, to support an MOU. The MOU should establish the requirements for data exchanged between the organizations, including the terms and conditions for the sharing of data and information resources in a secure manner, and specify the expected behavior from users who are given access to an interconnection.

Recommendations

We recommend that the Under Secretary, S&T, direct its Acting CIO to:

11. Complete supporting documentation required for the C&A of DHS' PIADC systems.
12. Work with DHS' CIO to ensure that USDA systems connected to DHS will be certified and accredited.
13. Approve and implement the IT contingency plans drafted for three of DHS' four operational systems. The plans should reflect any defined risks and threats to assets. Contingency plan testing results should be documented to ensure adequate IT services are available to sustain the PIADC's essential functions.
14. Develop an MOU between DHS and USDA to ensure that security requirements are documented and agreed to before DHS' systems are connected to USDA's network. The MOU should define the responsibilities for establishing, operating, and maintaining the security of the interconnection between DHS and USDA.
15. Establish an ISA between DHS and USDA for their interconnection requirements.

Management Comments and OIG Analysis

S&T concurred with recommendation 11. S&T IT Security has successfully completed certification efforts and obtained authority to operate (ATO) letters for all operational systems. All documentation has been uploaded into the DHS compliance system, Trusted Agent FISMA.

We accept S&T's response through its certification and accreditation of PIADC systems.

S&T concurred with recommendation 12. S&T has started to work with USDA counterparts in ensuring that any USDA system connected to DHS systems will be certified and accredited. This will be mandatory if there are any interconnections in the new PIADC network.

We accept S&T's response to work with USDA to ensure that connected systems have been certified and accredited.

S&T concurred with recommendation 13. Each system has a current signed Contingency Plan in place. Contingency test plans and results have been archived for the PIADC Tactical Communications System. Three other systems (to include PIADC Apple Cluster, PIADC Security System, and PIADC Building Management System) have signed contingency plans in place and testing will be completed during an April 15th ISSO visit to Plum Island.

We accept S&T's response regarding the approval, implementation, and testing of the IT contingency plans for the PIADC operational systems.

S&T concurred with recommendation 14. S&T will work with DHS Infrastructure to develop plans to create an MOU between DHS and USDA. All systems affected will be evaluated and a plan for certification of the USDA systems will be created by management.

We accept S&T's response to develop an MOU between DHS and USDA.

FOR OFFICIAL USE ONLY

S&T concurred with recommendation 15. Currently, an ISA is in draft form and being reviewed by USDA management. The ISA has been created for the interconnection of the PIADC AC system that is connected to the USDA infrastructure. The ISA encompasses all DHS requirements and management of the interconnection.

We accept S&T's response to establish an ISA between DHS and USDA for their interconnections.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Appendix A Purpose, Scope, and Methodology

The overall objective of this audit was to determine whether S&T has implemented effective physical security measures and adequate logical access controls over DHS' systems and data housed at PIADC. Specifically, we determined whether PIADC has implemented: (1) adequate physical security controls to safeguard personnel and prevent unauthorized access to, and the loss, theft, destruction, sabotage, or compromise of equipment, material, and sensitive information, and (2) adequate logical access controls to protect sensitive systems and data from unauthorized use, disclosure, disruption, modification, or destruction. We also evaluated whether PIADC's systems comply with FISMA requirements. In addition, we followed up on GAO's findings and recommendations regarding physical security at PIADC.

To identify whether physical security controls have been implemented to properly safeguard personnel, equipment and the facility, we analyzed the documents PIADC personnel provided. These documents included PIADC's physical security plan; standard operating procedures; post orders; Visiting Program policy; personnel security policies and procedures; O&M contract; corrective action plan; and COOP. We also interviewed PIADC, S&T, and contractor security personnel regarding the processes and procedures for granting and controlling physical access to Plum Island and PIADC facilities.

Our audit included an on-site evaluation of the physical security controls implemented for the ferry service; island grounds and the surrounding environment; main building, including the security control center; computer server room; and biocontainment areas. We also focused on the areas of concerns GAO previously reported. Based on a review of DHS and other federal and industry standards, we created a checklist to document our observations of the physical security controls in place at PIADC and the effectiveness of their implementation.

We conducted system security vulnerability assessments to determine whether adequate logical access controls have been implemented on the DHS systems located at PIADC. We also

FOR OFFICIAL USE ONLY

Appendix A Purpose, Scope, and Methodology

tested for unauthorized wireless access points and devices at PIADC.

We used Internet Security Systems' (ISS) Internet Scanner to conduct the system security vulnerability assessments. ISS' Internet Scanner provides an automated vulnerability assessment on servers, workstations, infrastructure devices, operating systems, routers/switches, firewalls, and applications to identify potential risks to an organization's network.

Fluke Optiview Network Analyzer was used to test for unauthorized wireless access points and devices. Fluke Optiview Network Analyzer monitors all 802.11a, b, and g channels to detect rogue access points and clients, which may compromise the performance and security of the enterprise networks. Fluke Optiview can identify unauthorized access points on a network, measure and plan access point locations, and verify wireless client connectivity from all locations.

We used Tenable Nessus to test the systems configured using Apple software. Tenable Nessus is a network vulnerability scanner for Linux, Berkeley Software Distribution, Solaris, Apple, and other systems. It currently performs more than a thousand remote security checks and can be used to scan a pre-defined range of Internet Protocol addresses to identify hosts and selected vulnerabilities.

Comprehensive Security Assessment (CSA) scripts were also used to test PIADC's [REDACTED] system running operating system [REDACTED] against the Defense Information System Agency (DISA) [REDACTED] Security Technical Implementation Guides. CSA scripts were developed and are currently maintained by the Department of Defense's (DoD) High Performance Computing Management Program.

DISA's Gold Disk, and Security Test Implementation Guides for [REDACTED] were used on standalone workstations to determine whether the recommended security and

b2, 7F
per S&T

FOR OFFICIAL USE ONLY

Appendix A
Purpose, Scope, and Methodology

b2, 7F
per S&T

configuration settings had been implemented and the local systems' security state. DISA Gold Disk assists system administrators in successfully securing [REDACTED] [REDACTED] This software program is designed as a tool for discovery and application recommended security and configuration settings and to assist in determining the state of local systems' security controls.

We analyzed the security posture of PIADC's system environment based on system diagrams we developed. Our system security assessments did not include PIADC's connection to DHS' Homeland Secure Data Network. Additionally, since PIADC's routers, switches, and firewalls were USDA-owned, we did not include perimeter security during our system vulnerability assessments of PIADC's systems, nor did we conduct vulnerability scans of the three systems in development that USDA transferred to S&T.

To determine whether PIADC systems complied with FISMA, we reviewed the FISMA requirements as well as DHS and National Institute of Standards and Technology (NIST) guidance. We also analyzed system documentation provided by S&T and PIADC personnel. This documentation included the TCS C&A package and draft system security plans, risk assessments, and self-assessments for the other three DHS systems. We also evaluated system POA&Ms and information security training attendance documentation and presentation slides. Additionally, we interviewed S&T and PIADC personnel regarding the status of the C&A of the other three DHS systems that were operational at PIADC, security awareness training, and specialized security training.

We conducted fieldwork at PIADC located on Plum Island, New York and coordinated our audit efforts with S&T headquarters. Fieldwork was completed from October 2006 through December 2006 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government

FOR OFFICIAL USE ONLY

Appendix A
Purpose, Scope, and Methodology

auditing standards. Major OIG contributors to the audit are identified in Appendix E.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for IT Audit, at (202) 254-4100, and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.

FOR OFFICIAL USE ONLY

Appendix B
Management's Response

Under Secretary for Science and Technology
U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

April 4, 2007

TO: Frank Deffer
Assistant Inspector General for Information Technology

FROM: Jay M. Cohen *Jay M. Cohen*
Under Secretary for Science and Technology

SUBJECT: Response to OIG Draft Report *Additional Physical, System, and Management Controls Can Enhance Security at Plum Island.*

Thank you for the opportunity to review and comment on the DHS OIG's Draft Report *Additional Physical, System, and Management Controls Can Enhance Security at Plum Island.*

S&T is responding to your memorandum dated March 7, 2007 which requests S&T to advise your office within 30 days of the progress of implementing the recommendations. Please refer to the attached documents which address the recommendations in your progress report. In addition, please find general comments to the draft report.

In our desire to further strengthen the enforcement of Security at Plum Island, we are supportive of and receptive to many of these recommendations.

If you have any further questions regarding these comments or corrective actions, please feel free to contact Cindy Christian, Administrative Officer at 202.254.5357.

Attachment

www.dhs.gov

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

Page 34

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Appendix B Management's Response

The Science and Technology Information Technology Security office has thoroughly reviewed the draft document *Additional Physical, System, and Management controls Can Enhance Security at Plum Island OIG-07-XX March 2007* and has prepared the following response to the Inspector General's (IG) recommendations.

The IG reported on **System Security Controls**. Within this section the IG has listed four recommendations. Below are the S&T IT Security department's response:

- In response to IG Recommendation #7:

S&T has planned a trip for the interim ISSO to go to PIADC for one week to begin the process of addressing the system vulnerabilities. All systems will be evaluated and the vulnerabilities will be mitigated. This will be completed before the implementation of the new Plum Island network.

- In response to IG Recommendation #8:

Currently, PIADC management is interviewing for a full time ISSO to fill the requirements of Plum Island information systems. The ISSO will be responsible for training all PIADC system personnel and implement DHS system administration policies and oversee the implementation of DHS system administration procedures.

- In response to IG Recommendation #9:

Currently, PIADC management is interviewing for a full time ISSO to fill the requirements of Plum Island information systems. The ISSO will be responsible for ensuring all DHS security policies are applied and also oversee the implementation of DHS procedures.

- In response to IG Recommendation #10:

Management is currently looking to fill the center director position.

The IG reported on **FISMA Compliance**. Within this section the IG has listed five recommendations. Below are the S&T IT Security department's response:

- In response to IG Recommendation #11:

S&T IT Security has successfully completed certification efforts and obtained authority to operate letters (ATO) for all operational systems. All documentation has been uploaded into the DHS compliance system Trusted Agent FISMA.

- In response to IG Recommendation #12:

S&T has started to work with USDA counterparts in ensuring that any USDA systems connected to the DHS systems will be certified and accredited. This will be mandatory if there are any interconnections in the new PIADC network.

FOR OFFICIAL USE ONLY

Appendix B Management's Response

- In response to IG Recommendation #13:

Each of the systems has a current signed Contingency Plan in place. Contingency test plans and results have been archived for the PIADC Tactical Communications System. Three other systems (to include PIADC Apple Cluster, PIADC Security System, and PIADC Building Management System) have signed contingency plans in place and testing will be completed during the April 15th ISSO visit to Plum Island.

- In response to IG Recommendation #14:

S&T will work with Infrastructure to develop plans to create an MOU between DHS and USDA. All systems affected will be evaluated and a plan for certification of the USDA systems will be created by management.

- In response to IG Recommendation #15:

Currently, an ISA is in draft form and being reviewed by USDA management. The ISA has been created for the interconnections of the PIADC AC system that is connected through the USDA infrastructure. The ISA encompasses all DHS requirements and management of the interconnection.

Responses to DHS – IG Report Recommendations, Physical Security, Page 15

Recommendation #1 Response

A review is being conducted of the Security Guard Post Orders that describe search requirements of personnel, packages and vehicles entering and exiting Plum Island. Appropriate changes will be made to reflect consistency in search requirements and training for the guard force will be conducted.

Recommendation #2 Response

In accordance with the Plum Island Security Plan, uncleared personnel are not permitted unescorted access to the server room. All uncleared personnel are monitored at all times while in the server room. Security and IT will implement a visitor sign – in log.

Recommendation #3 Response

A statement of work has been developed with the assistance of the Army Corps of Engineers, Electronic Security Center, Huntsville, Alabama, that captures the comprehensive physical security enhancements that will correct the deficiencies detailed in the IG Report. The services of an Architect / Engineering firm are in process of being solicited to develop the construction detail for soliciting bids on the work. A schedule for the completion of each phase is being developed.

FOR OFFICIAL USE ONLY

Appendix B Management's Response

Recommendation #4 Response

The update and revision of the COOP plan is an ongoing process. All pertinent risk assessment data will be considered in developing the final plan and its revisions. Separate from the COOP Plan, there are emergency operation and disaster recovery plans in place to deal with emergencies and unexpected events.

Recommendation #5 Response

See response to #3. This statement of work addresses all known security issues. The entire CAP as reported to Congress is refined and updated as new information becomes available and/or as tasks are implemented for completion. The first item addressed for any of the areas is to develop a statement of work with detailed cost and schedule for completion. DHS is utilizing a variety of in-house and contractor specialist to address each of the areas and plan the execution of the detailed projects.

Recommendation #6 Response

DHS continues to work on oversight of the O&M contractor for improved performance and quality of service. This is aided by now having an on-site contracting officer. In addition the contract will be up for re-bid in two years and the CO will address any significant changes required.

The following are general comments to the draft report provided to DHS S&T:

Comments to Draft IG Audit Report

1. Page 3, Background – 3rd Sentence, insert the word “authorized” between “and visitors.” Also, suggest inserting “DHS owned/operated” between by and ferry in that sentence. OIG: added “authorized” and “DHS-owned/operated.”
2. Page 5, 2nd Paragraph, foot-and-mouth is not zoonotic and doesn't “cause illness and death in humans”. Also, shouldn't the phrase, “introduction of animal diseases to the general population” say to the general animal population? Almost all studies on foreign animal diseases at PIADC are with non-zoonotics, the diseases affect animals and not humans. OIG: Revised.
3. Page 11, Server Room Security – 4th sentence, we believe there may have been some confusion on authorization by the IG Reps. The only incident the PIADC staff recalls during the visit was a case of maintenance personnel being escorted by another contractor working in the Engineering Department. That contractor, while not a federal employee, has all of the clearances and authorization necessary to be in the server room and to escort others there. OIG: Comment noted.

FOR OFFICIAL USE ONLY

Appendix B Management's Response

4. Page 16, Siemens System, 2nd Sentence. Note: In general, Siemens' technicians manage the Siemens system; however some operation support is also provided by FSSI trained personnel.
OIG: Added "contractors."
5. Page 32, PIADC Systems Chart— shows the security system as a component of the Proposed Plum Island Network. This is inaccurate. The security system is and will remain a stand alone system.
OIG: Appendix C was removed.
6. Page 33 – 36 Appendix D – This data is not helpful unless it is broken down by the system it applies to.
OIG: Technical staff was provided with individual system vulnerability reports.
7. Appendix C— appears to have PI net connecting all systems, but that is not the goal.
OIG: Appendix C was removed.
8. Page 19, PIADC Network Implementation Concerns Section also states that all systems will be connected on the PI network solution. While there will be DHS computers on the PI net there is no plan to connect any of the systems in this audit to the PI net.
OIG: Revised. Component indicated that all DHS systems may not be connected to the PI network, which may mitigate some of the risks associated with the vulnerabilities identified on those systems.
9. Page 20, Wireless Security Scan Section, USDA is referred to as a whole, and there is no differentiation between ARS, and APHIS networks. There are other locations where these two are grouped together as well. The problem is that while we do have DHS computers on the USDA-ARS network, there are no DHS computers on the APHIS network.
OIG: We are not focusing on the USDA network, only that there are DHS computers connected to another network that is not DHS-owned.
10. Page 20, Wireless Security Scans Section, it is stated that PIADC personnel were not aware whether there were wireless access points on the island. We did discuss the APHIS wireless access points prior to the wireless survey.
OIG: Revised.
11. Page 1, last sentence of second paragraph, whose field work, GAO or IG? If GAO the year is incorrect. If IG it was November, 2006.
OIG: OIG fieldwork ended December 2006. Our site visit was in November 2006.
12. Page 1, second sentence, third paragraph, which GAO recommendation not addressed?
Need clarification.
OIG: Addressed in the body of the report, pages 8 and 9.

FOR OFFICIAL USE ONLY

Appendix B Management's Response

13. Page 3, second paragraph, last three sentences, PIADC has always been under USDA. The Army Chemical Corp was never involved in foreign animal disease research or in PIADC. The Army occupied the island for a number of years (dating to late 1800's) prior to USDA and prior to PIADC.
OIG: Obtained from PIADC's website.
14. Page 5, last paragraph, the Corrective Action Plan (CAP) undertaken by DHS is much broader than security issues. Security is only one of five major areas, including environmental compliance and safety, documented in the FY2005 Report to Congress that outlines and documents the CAP. See page 13 of the report for further comments on the CAP.
OIG: Comment noted.
15. Page 13, third paragraph, "Still, the estimated cost for the major upgrades identified in the plan was \$56.1 million in 2004." We don't understand what this statement means, especially in the context of this paragraph. The CAP, again formally reported to Congress in FY05, did have a total cost estimate of \$56M. DHS has been implementing that Plan with funding every year since FY04. Many of the proposed actions have been completed. Through FY06, over \$30M had been budgeted and in FY07 an additional \$20M is budgeted. The final funding for the \$56M total is planned for FY08 and all activities in the CAP are scheduled for completion in FY09.
OIG: Revised.
16. Page 13, last paragraph, the January 2006 is incorrect. There has been an O&M contractor on the site ever since DHS took over responsibility in 2003. Confusion may have arisen because the current contract is on a calendar year basis with multiple option years.
OIG: Revised.

FOR OFFICIAL USE ONLY

Appendix C
Summary of Significant Security Vulnerabilities Identified and Potential Threats

Vulnerability	Patch Management	Identification and Authorization	System Integrity	Application Security	Threat
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

Appendix C
Summary of Significant Security Vulnerabilities Identified and Potential Threats

Vulnerability	Patch Management	Identification and Authorization	System Integrity	Application Security	Threat
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]				✓	[REDACTED]
[REDACTED]			✓		[REDACTED]
[REDACTED]		✓			[REDACTED]
[REDACTED]		✓			[REDACTED]
[REDACTED]		✓			[REDACTED]
[REDACTED]			✓		[REDACTED]
[REDACTED]			✓		[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]

b2,7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

Appendix C
Summary of Significant Security Vulnerabilities Identified and Potential Threats

Vulnerability	Patch Management	Identification and Authorization	System Integrity	Application Security	Threat
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]		✓			[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

Appendix C

Summary of Significant Security Vulnerabilities Identified and Potential Threats

Vulnerability	Patch Management	Identification and Authorization	System Integrity	Application Security	Threat
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]	✓				[REDACTED]
[REDACTED]			✓		[REDACTED]

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

Appendix C
Summary of Significant Security Vulnerabilities Identified and Potential Threats

Vulnerability	Threat			
	Patch Management	System Integrity Identification and Authorization	Application Security	
[REDACTED]	✓			[REDACTED]

b2, 7F
per S&T

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island

FOR OFFICIAL USE ONLY

Appendix D
Major Contributors to This Report

Information Security Audit Division

Edward G. Coleman, Director

Barbara Bartuska, Audit Manager

Tarsha Ross, Senior IT Auditor

Mike Horton, IT Specialist

Swati Mahajan, IT Specialist

Matthew Worner, Referencer

Advanced Technology Division

Vincent Feaster, Electrical Engineer, Space and Naval Warfare Systems
Command

Joseph Klein, Senior Security Analyst, Honeywell Technology Solutions, Inc.

FOR OFFICIAL USE ONLY

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary, Legislative and Intergovernmental Affairs
Assistant Secretary, Policy
Assistant Secretary, Public Affairs
Office of Security
Office of Privacy
CIO
Deputy CIO
Chief Information Security Officer
CIO, S&T
Deputy CIO & ISSM, S&T
Program Manager for Agriculture Security, S&T
Laboratory Operations Team Lead, Office of National Labs, S&T
Acting Director, PIADC
Security Manager, PIADC
GAO/OIG Liaison
Director, Compliance and Oversight Program
Audit Liaison, S&T
Audit Liaison, CIO
Director, Information Security Audit Division

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Physical, System, and Management Controls Can Enhance Security at Plum Island



Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.

