
DOI Trust Reform

*Interim Information Assurance Report and
Roadmap
For
TAAMS and BIA Data Cleanup*



CONFIDENTIAL

Limited Distribution

November 12, 2001



Limited Distribution Document

At the direction of the Department of Interior, Office of the Special Trustee for American Indians, distribution of this report has been limited. Reproduction, in any form, or further distribution of this report is expressly prohibited without prior written consent of the Office of the Special Trustee for American Indians.

Table of Contents

Information assurance includes all of the system, network and procedural tools and utilities that adequately protect confidentiality, integrity and availability of an organization's information. This report highlights a number of significant security weaknesses, therefore EDS is submitting this section as a separate addendum.

This is the third of three deliverable documents for the TAAMS and BIA Data Cleanup Assessment. DOI comments on the "Recommendations: For Comments' Report" returned as of November 8, 2001 have been considered in revising EDS' recommendations and the roadmap contained in this report. The report is labeled Draft to recognize that comments will be returned and edits incorporated and included in the "Final Report on DOI's Trust Reform Initiatives".

Table of Contents

Limited Distribution Document	2
Table of Contents	3
Summary Recommendations	5
Short Term Recommendations:	6
Long Term Recommendations:	7
Roadmap Summary	7
Detailed Recommendations	8
Immediately mitigate serious security vulnerability.....	9
Implement and enforce password management practices	10
Perform account management housekeeping functions	11
Deploy DOI agency wide Advice and Consent (Warning) Banner.....	12
Ensure service providers conform to BIA security requirements.....	12
Explicitly identify SLA information assurance expectations.....	12
Develop and test Disaster Recovery and Business Continuity plans	13
Hire and retain skilled staff in Network office.....	14
Complete security requirements documentation	14
Adopt certification and accreditation for TAAMS.....	15
Roadmap	17
Overview	18
Roadmap Activities	19
Appendix A - Detailed Findings	25
Information Assurance	26
Federal Systems Security Requirements	29
Contingency Plans	31
Security Requirements.....	32
Contractor Relationship.....	33
Operational Documentation	34
Human Resources	36
Identification & Authentication	37
Account Management	39
Firewalls	41
Auditing and Intrusion Detection	44
Data Integrity.....	45

Summary Recommendations

Summary Recommendations

The recommendations listed below are suggested solutions to the issues highlighted in Appendix A, Detailed Findings section of this report, which have been previously presented to BIA.

The recommended solutions are not intended to match one solution to one issue. One solution may address several issues or one issue may have several solutions. The ten solutions are organized into short-term recommendations and long-term recommendations. They are categorized this manner to allow the BIA to receive the most impact in the shortest period of time.

Short Term Recommendations:

- Immediately implement the following recommendations to mitigate serious vulnerabilities identified by EDS. See the Detailed Recommendations section for additional information.
 - Add firewalls to BIANET.
 - Implement an intrusion detection system (IDS) and perform proactive review of audits.
 - Periodically perform automated vulnerability assessments.
 - Develop procedures or plans to close the “backdoor”.
- Immediately implement and enforce password management practices which comply with BIA requirements and industry standards.
- Perform regular user account management housekeeping functions.
- Deploy DOI agency wide Advise and Consent (Warning) Banner in accordance with Public Law 99-474, DOI IRM Bulletin dated June 12, 2001, and DOI 375 DM, Chapter 19.

Recommendations: For Comments Report - Information Assurance

Long Term Recommendations:

- Ensure BIA internal and external service providers conform to BIA security requirements as well as to applicable regulations, departmental and industry practices in the area of information assurance.
- Ensure all Service Level Agreements (SLA) explicitly identify information assurance expectations.
- Develop and test Disaster Recovery and Business Continuity plans for the BIANET.
- Hire and retain skilled and qualified staff to fulfill the operational commitments required of the BIA OIRM IT network office.
- BIA needs to complete the security requirements documentation for TAAMS and include the security requirements in the standard testing process.
- Adopt the “authority to process” certification and accreditation for TAAMS.

A detailed discussion of each solution follows in the Detailed Recommendations Section of this report. It is understood that no solution can guarantee 100% risk mitigation, but the residual risk can be lowered.

Roadmap Summary

The roadmap that follows illustrates the timeframes in which information assurance activities can commence, the anticipated duration of those activities and any dependencies that exist between dependencies.

It is expected that all of these activities can be completed within one calendar year. It should also be noted, however, that several of these activities are urgent and need to be completed rapidly in order to assure the security of TAAMS-related business processes and data. Those activities are listed below:

- Immediately mitigate serious security vulnerabilities;
- Implement and enforce password management practices;
- Perform account management housekeeping functions; and
- Deploy the DOI agency-wide Advise and Consent (Warning) banner.

When these obligations are fulfilled, the Department will issue an interim ‘authority to process’ letter for TAAMS, providing additional time to comply with the remaining obligations.

Detailed Recommendations

The information contained in this section provides supplementary details of the high-level recommendations stated in the Executive Summary.

Detailed Recommendations

Immediately mitigate serious security vulnerability

Immediately implement the following recommendations to mitigate serious vulnerabilities identified by EDS. Risk mitigation recommendations are:

- Add firewalls to BIANET – Three separate firewall recommendations are made:
 - (1) Add a firewall on the BIANET between the BIANET and the Internet Service Provider (ISP);
 - (2) Add a firewall on the ATS network between BIANET and TAAMS;
 - (3) Add a firewall on the ATS network between the ATS corporate LAN and TAAMS to increase isolation of the BIA TAAMS application from the ATS corporate LAN

Further discussion of firewalls is in Appendix A, Detailed Findings, Firewalls.

- Implement an intrusion detection system (IDS) and perform proactive review of audits. The IDS is a system that monitors for attacks on the network and produces an audit trail. Combining firewalls and IDS together helps implement layered security. The review of audits logs produced by the firewalls, IDS, operating systems, and applications needs to occur on a regular basis rather than an exception basis. Further discussion is in Appendix A, Detailed Findings, Auditing and Intrusion Detection.
- Periodically perform penetration tests or automated vulnerability assessments. The penetration tests or automated vulnerability assessments are methods use to test the security environment, verify the configuration of the security mechanisms (e.g., firewalls, IDS, gateways, and routers) and verify the security mechanisms are performing as expected.
- Develop procedures and plans to close the “backdoor”. The “backdoor” in the software application allows direct access to TAAMS data by circumventing the monitoring and auditing process. It is identified in Appendix A, Detailed Findings, Data Integrity.

Recommendations: For Comments Report - Information Assurance

Implement and enforce password management practices

Immediately implement and enforce password management practices which comply with BIA requirements and industry standards. Password management includes enforcing the following:

- Identification and Authentication – User ids and passwords for end-users, privileged users, and hardware/software functions.
- Access Control Lists – Filters for both in-bound and out-bound traffic through routers, gateways, firewalls, etc.
- Authorization – User profiles and how they are determined or assigned.
- Change requirements – Frequency of password changes (e.g., industry standard is every 30 or 60 days), and password reuse policies.
- Education – Training the user on responsibilities that go hand-in-hand with access to the information. It also includes educating the user on penalties for misuse of their password or the information they access (e.g., loss of employment, fines and jail).
- Lockout attempts – Industry standard of user lockout after three invalid attempts and requiring the security administrator to reset the user manually.
- Password database encryption – Passwords must be encrypted.
- Administrator Accounts – The security on administrator accounts must be more stringent (e.g., limit the number of accounts and change passwords more frequently than end-user accounts) because they have a high level of privileges.
- Access Control List (ACL) Reporting Tool – A tool that is used to validate and manage the access control list on routers, gateways, firewalls, etc.
- Secure and Manage Event Logs – Protection of the event logs to prevent tampering. Event logs are key instruments in any potential security incident investigation.
- Strong password policy – Define the structure of the password to include the number of characters, content of the password (alpha, numeric, alphanumeric, special characters), and what is used for a password. Personal identifiers such as family names, makes of cars, birthdays, sports teams are prohibited as well as words found in a dictionary, and other easily guessed words.

Perform account management housekeeping functions

Perform regular user account management housekeeping functions. These functions include:

- Deleting user privileges after an extended period of inactivity. These would include access privileges established but never used and privileges associated with personnel who have terminated employment. When the user terminates employment, their files should be moved to a limited access location and their privileges revoked. Standard practice is after 30 to 60 days of inactivity access privileges are revoked.
- Suspend the access privileges of personnel who take extended leaves of absence like maternity leave, sabbaticals, long vacations, etc.
- Ensure that business user authority is segregated to assure the principles of least privilege and separation of duties has been applied. Individuals with the ability to make changes that affect legal interests should not also have the ability to approve those changes.
- Recertify users annually. Managers need to certify that the user still needs access to the system at the level currently on file. This will help identify situations where personnel who have changed jobs but stayed within the agency or terminated employment but the system administrator was never notified
- Implement automated logoffs after a period of inactivity and at the end of the workday. Automated logoffs allows for a more complete backup of files, as a file that is left open is not normally backed up and terminates any open connection.
- Require screen timeouts after inactivity to prevent unauthorized use of the system. Standard practice is to timeout after 10 to 15 minutes of inactivity.
- Require screensavers with the password option activated

Recommendations: For Comments Report - Information Assurance

Deploy DOI agency wide Advise and Consent (Warning) Banner

Deploy DOI agency wide Advise and Consent (Warning) Banner in accordance with Public Law 99-474, DOI IRM Bulletin dated June 12, 2001, and DOI 375 DM, Chapter 19.

Advise and Consent Banners are recommended for a variety of reasons that would both legally protect the BIA and ATS (from potential lawsuits) and assist BIA and ATS (in prosecuting unauthorized use). Justification for and legal consequences of not having an Advise and Consent Banner include the host organization could be sued for invasion of privacy if they did active monitoring of user activities. Likewise, without the banner you cannot successfully prosecute a hacker that breaks into the system.

Based on EDS findings, a sample Advise and Consent Banner has been provided by the BIA CIO Office to the TAAMS Project Office.

Ensure service providers conform to BIA security requirements

Ensure BIA internal and external service providers conform to BIA security requirements as well as to applicable regulations, departmental and industry practices in the area of information assurance. Two specific recommendations in this area are:

- Restructure the ATS contract to adhere to regulatory, departmental and industry practices.
- Review Federal, DOI, OST, and BIA regulations and guidelines as well as industry practices. The goal would be to identify deficiencies in the existing agreements. These regulations and guidelines are identified in the Appendix A, Detailed Findings, under the heading, Federal Systems Security Requirements.

Explicitly identify SLA information assurance expectations

Ensure all Service Level Agreements (SLA) explicitly identify information assurance expectations. These expectations must have performance metrics that ensure confidentiality, integrity, and availability in the TAAMS environment. At a minimum, the SLAs must have the following components:

- Manageability of network security – This would specifically identify who is responsible for the management of network security and what their roles and responsibilities are.
- System availability and responsiveness – Indicate a specific amount/percentage of TAAMS availability that must be maintained and reasonable response time windows for all core business transactions.

Recommendations: For Comments Report - Information Assurance

- Liquidated damages – Indicate any penalty that might be incurred by the contractor if the system/data is unavailable for a defined period of time.
- Accuracy – This relates to the integrity of the data in that it was entered correctly when originally entered into the system and has not been changed through unauthorized means since that time.
- Data Recovery – Ensure files on backup tapes can be restored, that mistakenly deleted files can be restored, and that user access is available in the event of a major disaster.

Develop and test Disaster Recovery and Business Continuity plans

Develop and test Disaster Recovery and Business Continuity plans for the BIANET. BIA needs to develop Disaster Recovery and Business Continuity plans to support the business needs of their users in the case of a catastrophic emergency. After the plans are developed they must be kept up to date and periodically executed in test mode.

Some common processes and procedures that need to be documented in the plan are:

- The events or system disaster timeframes that determine when the plans are executed.
- System and data backup locations and procedures to restore the critical business support systems.
- Each business process and its supporting information systems needs to be scrutinized to determine if and when it becomes critical to operations.
- Prioritizing the restoration of critical processes to support the critical business processes.
- Locating and contracting for alternate site processing in the event the primary site is unavailable. The contracts should include service level agreements and testing schedules so the transition to an alternate site could proceed smoothly.
- Identify the logistical requirements to move personnel, files, documentation, and supplies to and from the alternate site(s). This requires detailed documentation, identifying critical personnel, travel needs and alternatives, funding requirements, supplies, and documentation needed at the off-site location.

Hire and retain skilled staff in Network office

While the DOI may choose to outsource some or all of their datacenter operations to a third party, information assurance functions need to be performed by a separate and internal organization. This strategy adheres to the 'segregation of responsibilities' policy and provides the greatest degree of integrity for IT services and the data those services manage. The Department should, therefore, hire and retain skilled and qualified staff to fulfill the operational commitments required of the BIA OIRM IT network office. Without proper staffing in the BIA OIRM IT network office, the security of the TAAMS information traversing the BIANET could be in jeopardy. In addition to current operational functions being performed, the following security related functions should also be performed:

- System Maintenance
- System Software Upgrades/Patches
- System Security Patches
- System Security Audits
- Capacity planning

Complete security requirements documentation

BIA needs to complete the security requirement documentation for TAAMS and include the security requirements in the standard testing process. The security requirements documentation when used effectively ensures a proactive security attitude during the entire life cycle of the system. It also establishes the minimum acceptable level of security to ensure adequate data availability, protection, integrity and confidentiality.

The security requirements and mechanisms to produce this secure environment need to be documented, validated, tested, and approved. This documentation is normally found in:

- System Security Requirements Matrix– A chart or spreadsheet that summarizes the security design document in a graphic representation. It contains information indicating what the security requirement is, where it was derived from, where it was incorporated into the system/application, when it was incorporated, when it was tested, and if it passed the test.
- System Security Design Document– A description of the minimum requirements provided for an information technology system and how they will be implemented to maintain an acceptable level of security.

Recommendations: For Comments Report - Information Assurance

- System Security Plan (A plan outline can be found in NIST Special Publication 800-18.)– A formal documentation of the in-place and planned security mechanisms or tasks required to meet the system security requirements.
- System Security Test and Evaluation Plan/Tests/Report– The plan and tests detail how the security features/mechanisms are to be examined and under what specific scenarios and, and the report is the result of the analysis of the examination output. A test and evaluation to determine that the security features/mechanisms of an information technology system are implemented as designed. This includes hands-on functional testing, penetration testing, and verification.

Adopt certification and accreditation for TAAMS

Adopt the “authority to process” certification and accreditation for TAAMS. ATS management needs to certify that TAAMS meets or exceeds all prudent security measures. They should structure an internal examination using the Federal government “Authority to process” certification and accreditation approach. After performing this examination, both ATS management and DOI should review, accept, and sign off on the identified risks and authorize the operation of the system. The following documentation should be produced prior to performing the assessment.

- System Security Review/Risk Assessment Report – A management tool which provides a systemic approach for determining the relative value and sensitivity of information technology assets, assessing vulnerabilities, assessing loss expectancy or perceived risk exposure levels, assessing existing protection features, and additional protection alternatives, or acceptance of risks and documenting the management decisions.
- System Security Requirements Trace ability Matrix– A chart or spreadsheet that summarizes the security design document in a graphic representation. It contains information indicating what the security requirement is, where it was derived from, where it was incorporated into the system/application, when it was incorporated, when it was tested, and if it passed the test.
- System Security Test and Evaluation Plan/Tests/Report– The plan and tests detail how the security features/mechanisms are to be examined and under what specific scenarios. The report is the result of the analysis of the examination output. A test and evaluation to determine that the security features/mechanisms of an information technology system are implemented as designed. This includes hands-on functional testing, penetration testing, and verification.

Recommendations: For Comments Report - Information Assurance

- Computer Security Awareness Training Program– An established and on-going program within an organization to educate computer users at all levels (i.e., end-users, technical staff, managers, and executives) of protective measures intended to ensure a state of inviolability from hostile acts and influences, design deficiencies, system/component failure/malfunctions, or unintentional misuse.

The letter authorizing system operation establishes the system security baseline, which needs to be re-evaluated as part of any major hardware or software changes requested to the system.

Roadmap

The TAAMS and BIA Data Cleanup Information Assurance Roadmap identifies the activities, together with their timing and dependencies, required to implement the recommendations described throughout the *“Detailed Recommendations”* section above.

Roadmap

The Roadmap section in this report reviews the following topics:

- Overview
- Roadmap Activities

Overview

The high-level and detailed recommendations described in the report above address each of the major highlights and concerns identified during EDS' assessment of the TAAMS and BIA Data Cleanup subprojects. They do not, however, describe the sequence in which each activity (recommendation) should be executed, nor do they describe interdependencies, effort or performance considerations that must be monitored in order to ensure smooth progress towards Trust Reform objectives. Each of these issues is described in the roadmap section below:

- The duration of that activity;
- Key interdependencies representing relationships with other high-level recommendations;
- Detailed recommendations, or tasks, that identify specific steps required to implement the recommendation;
- Detailed interdependencies representing relationships between activities within the same high-level recommendation. These dependencies are identified to provide sub-project managers with an appropriate view of the anticipated contribution that each task makes to the overall effort; and
- Performance considerations that provide both Trust executives and sub-project managers with insight into the key issues, measures, decision points and/or milestones that must be monitored in order to assure a successful implementation.

The graphic on the right illustrates the relationship between each recommendation and the core change components and the means by which activity start dates and duration are indicated throughout the body of the roadmap. The '1Q' to the left of the colon indicates that this activity is expected to commence in the first (1st) quarter of the Reform program. The '3-6 months' indicates that completion is anticipated to require from three (3) to six (6) months.

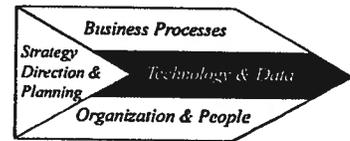


Recommendations: For Comments Report - Information Assurance

Roadmap Activities

I. Immediately mitigate serious security vulnerabilities. 1Q: < 3 months

Immediately implement the following recommendations to mitigate serious vulnerabilities identified by EDS. See the Detailed Recommendations section for additional information.

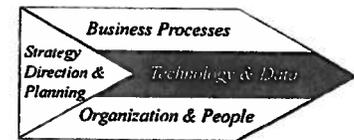


Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Deploy the firewalls detailed in the Appendix of this report.	<3 months
Implement an intrusion detection system (IDS) and perform proactive review of audits.	<3 months
Periodically perform automated vulnerability assessments (AVAs).	<3 months
Develop procedures or plans to close the "backdoor".	<3 months

II. Implement and enforce password management practices. 1Q: < 3 months

Immediately implement and enforce password management practices which comply with BIA requirements and industry standards.



Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Develop and distribute appropriate BIA policies.	<3 months
Ensure separation of duties between system, network, and security administrators.	<3 months
Provide appropriate training to the system, network, and security administrators.	<3 months

Recommendations: For Comments Report - Information Assurance

III. Perform account management housekeeping functions.

1Q: < 3 months



Perform regular user account management housekeeping functions.

Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Develop and distribute appropriate BIA information assurance policies and procedures.	<3 months
Ensure separation of duties between system and security administrators.	<3 months
Ensure separation of authority between business users with the authority to make changes and business users with the authority to approve changes.	<3 months
Provide appropriate training to the system and security administrators.	<3 months

IV. Deploy DOI agency wide Advise and Consent (Warning) Banner.

1Q: < 3 months



Deploy DOI agency wide Advise and Consent (Warning) Banner in accordance with Public Law 99-474, DOI IRM Bulletin dated June 12, 2001 and DOI 375 DM, Chapter 19.

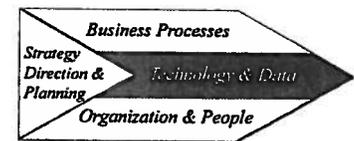
Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Verify that the TAAMS and BIANET Advise and Consent Banner has been deployed in accordance with BIA policy.	<3 months

Recommendations: For Comments Report - Information Assurance

V. Ensure service providers conform to BIA security requirements.

1Q: 6-9 months



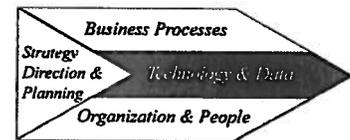
Ensure BIA internal and external service providers conform to BIA security requirements as well as to applicable regulations, departmental and industry practices in the area of information assurance.

Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Applicable personnel (contracting officer, COTR, program manager) familiarize themselves with the statutes, regulations, and guidelines.	<3 months
Restructure service provider contracts to conform to identified requirements in applicable statutes, regulations, and guidelines.	3-6 months

VI. Explicitly identify SLA information assurance expectations.

1Q: 6-9 months



Ensure all Service Level Agreements (SLA) explicitly identify information assurance expectations. These expectations must have performance metrics that ensure confidentiality, integrity, and availability in the TAAMS environment.

Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Applicable personnel (contracting officer, COTR, program manager) familiarize themselves with the statutes, regulations, and guidelines.	<3 months
Review, restructure, or establish SLAs to conform to identified requirements with specific metrics.	3-6 months

Recommendations: For Comments Report - Information Assurance

VII. Develop and test Disaster Recovery and Business Continuity plans.

1Q: 9-12 months

Develop and test Disaster Recovery and Business Continuity plans (DRP and BCP) for the BIANET. BIA needs to develop Disaster Recovery and Business Continuity plans to support the business needs of their users in the case of a catastrophic emergency. After the plans are developed they must be kept up to date and periodically executed in test mode.



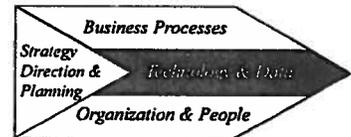
Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Identify the scope/boundary of the DRP and BCP as well as the location of an alternate site(s).	<3 months
Develop contract, SLA, or memorandum of agreement (MOA) with the alternate site(s) host(s).	3-6 months
Develop the DRP and BCP, identifying specific teams, responsibilities, disaster declaration timeframes, and logistical information.	6-9 months
Test the DRP and BCP and update the plans with "lessons learned" from the test.	<3 months

VIII. Hire and retain skilled staff in Network office.

1Q: 9-12 months

While the DOI may choose to outsource some or all of their datacenter operations to a third party, information assurance functions need to be performed by a separate and internal organization. This strategy adheres to the 'segregation of responsibilities' policy and provides the greatest degree of integrity for IT services and the data those services manage. The Department should, therefore, hire and retain skilled and qualified staff to fulfill the operational commitments required of the BIA OIRM IT network office.



Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Identify the additional positions required.	<3 months
Advertise for and hire skilled and experienced personnel.	9-12 months

Recommendations: For Comments Report - Information Assurance

IX. Complete security requirements documentation.

1Q: 9-12 months

BIA needs to complete the security requirement documentation for the portion of TAAMS that will be immediately deployed, and include the security requirements in the standard testing process. The security requirements documentation when used effectively ensures a proactive security attitude during the entire life cycle of the system. It also establishes the minimum acceptable level of security to ensure adequate data availability, protection, integrity and confidentiality.

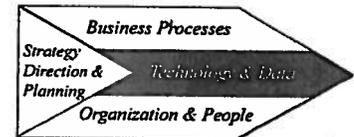


The security requirements and mechanisms to produce this secure environment need to be documented, validated, tested, and approved.

Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
TAAMS Project Management Office continues their efforts to discover and retrofit the security requirements to TAAMS.	6-9 months
Adequately test the security requirements/mechanisms in place to ensure they perform as expected.	<3 months

1Q: 9-12 months



Recommendations: For Comments Report - Information Assurance

X. Adopt certification and accreditation for TAAMS.

Adopt the “authority to process” certification and accreditation for TAAMS. ATS management needs to certify that TAAMS meets or exceeds all prudent security measures. They should structure an internal examination using the Federal government “Authority to process” certification and accreditation approach. After performing this examination, both ATS management and DOI should review, accept, and sign off on the identified risks and authorize the operation of the system. The following documentation should be produced prior to performing the assessment.

This activity depends upon
Activities I. – IX.

In the following manner

All previous activities must be completed before the final ‘authority to process’ letter for TAAMS can be issued. An interim ‘authority to process’ letter can be issued after the completion of the first four (4) activities.

Scope and Duration

<i>Task(s)</i>	<i>Task Duration</i>
Developed documentation to assess the current risk environment for TAAMS. (Refer to Appendix A for details of the documentation that has been developed vs what needs to be developed.	6-9 months
Review developed documentation to assess the current risk environment for TAAMS.	<3 months
ATS management, together with BIA determines whether or not to accept the risk and issue an “authority to process” letter or TAAMS.	<3 months
Review the impact of major business process and IT changes on the security environment to ensure that it has not been compromised.	Ongoing

Appendix A - Detailed Findings

Appendix A: Detailed Findings

Appendix A: Detailed Findings in this report reviews the following topics:

- Information Assurance
- Federal System Security Requirements
- Contingency Plans
- Security Requirements
- Contractor Relationships
- Operational Documentation
- Human Resources
- Identification and Authentication
- Account Management
- Firewalls
- Auditing and Intrusion Detection
- Data Integrity

Information Assurance

Definition – Ensuring that an organization's information has adequate confidentiality, integrity and availability.

Goal - Business and technical processes and information will be adequately protected at all times.

Recommendations: For Comments Report - Information Assurance

The three pillars of information assurance are confidentiality, integrity and availability. They are defined as:

- Confidentiality is ensuring that only authorized individuals have access to information.
- Integrity is ensuring that data has not been tampered with, altered, or contaminated.
- Availability is having information obtainable when it is wanted or needed.

This risk analysis represents a “snap shot in time” of TAAMS taken during the data collection phase of the report. The overall data collection phase for information assurance included the period from August 10, 2001 through September 19, 2001. Data collection from ATS in Dallas was accomplished during the period of August 20, 2001 through August 24, 2001.

It is important to recognize that no security procedure is 100 percent guaranteed to eliminate all risks. If the additional safeguards, when recommended in this risk analysis are not implemented, the result could be corruption or destruction of data. In addition it could lead to the disclosure of sensitive unclassified information, or denial of service to the users who require the information on a frequent basis.

Overall, at the time of the review, EDS found that there are significant confidentiality and integrity risks to information in the TAAMS system. The current security safeguards protect against casual or inadvertent access to information. The system is not well protected against deliberate intrusion. Adequate security requirements, tools and processes have not been instituted using a layered security approach. A layered security approach would include:

- Firewalls
- Intrusion Detection
- Active Systems Audits
- Effective Identification and Authentication Processes

BIA has recognized some of the issues associated with information assurance. At the time of the review, BIA was in the process of obtaining a firewall and intrusion detection software. This is a good start, but a complete information assurance approach is required.

To examine the information assurance aspects of the TAAMS systems EDS examined the following:

- Contingency Plans
- Security Requirements

Recommendations: For Comments Report - Information Assurance

- Contractor Relationship
- Operational Documentation
- Human Resources
- Identification and Authentication
- Account Management
- Firewalls
- Auditing and Intervention Detection
- Data Integrity

This section starts with a description of legal federal system security requirements and guidelines. It then reviews the areas listed above. The order of presentation is random and has no correlation to the level of risk associated with each theme or observation.

Recommendations: For Comments Report - Information Assurance

Federal Systems Security Requirements

TAAMS, as a federal government system, is required to comply with the regulations listed below:

- Computer Security Act of 1987 (Public Law 100-235)
- Paperwork Reduction Act (Public Law 93-511)
- Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control
- OMB Circular A-127, Financial Management Systems
- OMB Circular A-130 Management of Federal Information Resources

The following are recommended Federal Guidelines that may be followed in an Information Assurance Program:

- National Institute of Standards and Technology (NIST) Special Publication 800-10, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST Special Publication 800-18, A Guideline for Developing Security Plans for Information Technology Systems
- NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST Special Publication 800-30, Risk Management Guide (Draft June 2001)
- NIST Special Publication 800-31, Intrusion Detection Systems
- National Security Telecommunications and Information Systems Security Committee (NSTISSC) Number 1000, National Information Assurance Certification and Accreditation Process (NIACAP)

Recommendations: For Comments Report - Information Assurance

- Federal Information Processing Standards Publication (FIPS Pub) 31, Guidelines for ADP Physical Security and Risk Management
- FIPS Pub 73, Guidelines for Security of Computer Applications
- FIPS Pub 83, Guideline on User Authentication Techniques for Computer Network Access Control
- FIPS Pub 87, Guidelines for ADP Contingency Planning
- FIPS Pub 102, Guidelines for Computer Security Certification and Accreditation
- FIPS Pub 112, Password Usage
- FIPS Pub 191, Guidelines for the Analysis of Local Area Network Security

Contingency Plans

Definition – A plan to mitigate effects of an adverse event that may occur.

Goal – To try to ensure continuity of business operations in the event of an anomaly.

EDS Observations and Findings

During interviews with the ATS personnel it was stated that there was a contingency plan for TAAMS and that it had been tested at COMDISCO alternate facilities.

ATS provided EDS with reports containing the results of two contingency plan tests conducted in December 1999 and June 2000. This proactive stance on contingency planning and testing follows both best business practices and federal guidelines.

BIA has indicated that they do not have a contingency plan.

Impact and Importance

A proven (tested) contingency plan would allow TAAMS to remain operational within the 48-hour downtime contractual limit. This would enable BIA to continue to discharge its fiduciary responsibilities to individual Indians, Indian Tribes, and other interested parties.

Lack of a contingency plan for BIANET places availability of information at risk if the network is disrupted due to a problem. A contingency plan for BIANET would include options for use of alternate networks and for replacement of failed network components.

Recommendations: For Comments Report - Information Assurance

Security Requirements

Definition – That which is necessary to ensure that only authorized people have access to the parts of a system that are required for their work.

Goal – To ensure the system is protected from unauthorized access.

EDS Observations and Findings

Discussions with a member of the TAAMS Project Office indicated that a “discovery” process was currently underway to produce a security requirements matrix for TAAMS and there was reason to believe the TAAMS application design documents did not include the security requirements.

Impact and Importance

Security requirements usually contain the overall system design document or a separate security design document. The design documentation generally would also contain a chart consisting of several pages outlining what the specific security requirements were, where they were derived from (law, regulation, guideline, etc.), where they should be or are functionally placed within the system. It would also contain information on how they should be tested, if the security requirements had been tested, and if they passed the test. Without documented security requirements there is no guarantee that information assurance has been adequately addressed to reduce the threat to the system and mitigate risks involving the confidentiality and integrity of data stored, process, or transiting the system, or the availability of the system itself.

Contractor Relationship

Definition – Description of the terms and conditions between the contractor and DOI as it relates to TAAMS software.

Goal – To maintain a proper business relationship between these two entities

EDS Observations and Findings

The contractual relationship between DOI and ATS is not clearly defined. Over time the relationship between ATS and DOI has changed from COTS product outsourcing provided into a relationship between a service provider with custom software and service recipient. The terms of the COTS product outsourcing relationship are not the same as MOTS or customized software. This leaves many items open for dispute. It is unclear what the rights and responsibilities are in the changed relationship. Upon termination or completion of the contract it is not clear what DOI would receive in terms of executable software, source code, and data. It is also unclear how the transition to a new environment would take place. There is no COTS product to move to another provider.

TAAMS, as an important part of the Trust Reform Project, needs meticulous oversight and management. BIA must be very specific and detailed in any contractual requirement it levies on the contractor.

Impact and Importance

The unclear nature of the relationships in the TAAMS contract creates a situation where business continuity may be in jeopardy. BIA has a fiduciary responsibility to protect the information that is in TAAMS and ensure that access is limited to authorized personnel only, the data integrity remains intact, and the data is available when needed. The contractual relationship between ATS and DOI should mitigate the risks by clearly articulating the rights and responsibilities of each party to the contract.

Recommendations: For Comments Report - Information Assurance

Operational Documentation

Definition – Manuals and other literature, which describes day-to-day and extraordinary processes and procedures.

Goal – To provide information required to operate systems properly and efficiently

EDS Observations and Conclusions

EDS Reviewed ATS documentation in accordance with National Information Assurances Certification Process (NIACP) requirements and found that ATS had the following:

- Data Center Security Plan,
- Physical Security Implementation Guidelines,
- Security Positions Identified in Job Descriptions,
- Data Center Standard Operational Procedures,
- TAAMS Disaster Recovery Program, and
- TAAMS Disaster Prevention and Recovery Plans and Procedures.

ATS was missing:

- Information System Security Requirements or Requirements Traceability Matrix,
- Information System Security Test and Evaluation Plan and Procedures,
- Information System Rules of Behavior,
- Information System Security Plan,
- Security Education, Training, and Awareness Plan,
- Information System Certification and Accreditation Statements, and
- Industry standard recommended security documentation for an operational IT system.

Recommendations: For Comments Report - Information Assurance

At the time of the EDS on-site visit to the contractor location, ATS was in the process of developing a Corporate Safety Plan which would include both physical and computer security and was in draft review and expected to be finalized by the end of October 2001. It is understood that ATS is progressing towards developing the needed 'living' documentation for an operational information system and that this will be an on-going task during the life cycle of the system.

A suggested certification and accreditation process is contained in the National Information Assurance Certification and Accreditation Process (NIACAP) (NSTISSC Instruction No. 1000). The NIACAP was issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and is recommended for federal government agencies and those that support federal agencies. NIACAP discusses the standard processes that can be used and the documentation needed to support the process.

Impact and Importance

Proper documentation is required to ensure that all aspects of information assurance have been thoroughly considered and documented. Management should be made aware of the potential risks, mitigation strategies and safeguards in place, and any residual risk, so that informed decisions about the security and operation of the information system can be made. Appropriate documentation needs to be available to the operations, maintenance, and user staff for the proper use and upkeep of the TAAMS information, application, and hardware.

Recommendations: For Comments Report - Information Assurance

Human Resources

Definition – A body of persons within an organization necessary to fulfill required functions.

Goal – Provide adequate personnel to perform all duties efficiently.

EDS Observations and Findings

BIA OIRM IT network office has insufficient resources (staff) to perform the roles required for an adequate information assurance program. BIA OIRM staff indicated that there are only three individuals performing network system administrator tasks. The move of the BIA Data Center from Albuquerque, NM to Reston, VA resulted in a loss of manpower when most employees chose not to relocate. The loss of 17 system administrators has put those administrators that are available in a 'fighting fires' mode. Therefore, critical functions such as, monitoring of system logs and monitoring of system and security patches/updates, are not being performed.

An effective information assurance program serves to mitigate potential security incidents and reduce damage to BIA's reputation.

Impact and Importance

Human resources are of particular importance to ensure information assurance. Although much of the routine work will be performed automatically, the interpretation of the reports and the determination of subsequent actions will require well-trained people. Without adequate numbers of such personnel, the quality of information could be compromised.

Identification & Authentication

Definition – Defines how the IT system recognizes an individual and verifies the individual's authorization to receive specific categories of information and perform specific functions.

Goal – To ensure those who should have access to a system do have access and those who are unauthorized do not have access.

EDS Observations and Findings

Password management for TAMMS directly contradicts industry standard practices, legislative and federal standards for compliance in the construction, use, and maintenance of passwords.

The potential presence of non-BIA related users profiles on the IBM AS/400, BIA dedicated system, opens the system to potential for unauthorized access.

There were four distinct password management issues that were found:

- Shared passwords were used during the TAAMS application demonstration (ATS, Dallas, TX).
- User codes corresponded to the password on the TAAMS application (Reston, VA) (ATS induced).
- The contract between BIA states in the Statement of Work, Section C, Paragraph C.4.8.2. (2) includes the following mandatory requirement: "The system shall require users to change their passwords at least every 60days. ATS says the functionality is available but was not requested and therefore not implemented.
- There were conflicting perceptions on whether or not ATS received direction from BIA on password changes.

Inconsistencies were noted in comments received during two interview sessions.

Participant(s) in one interview session conveyed information that non-BIA ATS client profile information was migrated from the shared IBM AS/400 mainframe to the BIA dedicated IBM AS/400 mainframe. During another interview session it was noted that only BIA user profile information was migrated from the shared mainframe to the BIA dedicated mainframe and that the system was tested to ensure the accuracy of that migration.

Recommendations: For Comments Report - Information Assurance

Impact and Importance

It is imperative that the ability to protect BIA information be preserved. BIA information must be protected from modification or destruction of data, disclosure of sensitive unclassified information, or denial of service to the users who require the information on a frequent basis. The concepts of least privilege and need-to-know must also be followed.

Several NIST Special Publications and FIPS Publications discuss the issues concerning strong password management and that in most information systems; passwords are used for the user's initial entry into the information system.

Traditionally, information system passwords are known as the first line of defense security mechanism for gaining access. The manner in which ATS manages passwords is ineffective and is susceptible to attack methods such as social engineering, plain old guessing and an ability to hack the network and steal user passwords. Password protection is only effective if both a strong technology is employed and policy is implemented to assure proper use. The reliability of an information system is only as good as its weakest component.

BIA personnel are under the impression that there is no function that allows for the changing of passwords on the TAAMS system by users. The TAAMS developer has indicated that unless the user specifically requested authority to change passwords when the user account was established, the authority was not given. The user code/password combination is the primary means of protecting the sensitive Privacy Act and financial information contained within TAAMS. The security of a passworded system is dependent upon keeping passwords secret. Currently, TAAMS passwords are never changed and are the same as the individual user's user code.

The IBM AS/400 mainframe should only contain BIA related user profiles and not users from other ATS client organizations. The possibility of unauthorized clients to view or access BIA data compromises the confidentiality and integrity security principles. If external clients are able to obtain BIA information via this method, it jeopardizes security protections.

Account Management

Definition – Defines how user accounts are managed and includes, but is not limited to: deleting old users, establishing new accounts, ensuring the concept of least privilege, logon and consent banners, lockout and timeout features.

Goal – To provide access to the system(s) using proper security.

EDS Observations and Findings

There are no provisions in the TAAMS application for deleting obsolete accounts due to inactivity or termination of duties/employment. There is no computer notice and consent log-on banner (warning screen) upon entry to the ATS network. During data collection, the software vendor informed EDS that there have been no requirements from the government for this feature. The developer also indicated that previous BIA Security Officers has not wanted accounts actually deleted/erased but preferred accounts to be revoked/suspended with a notation of when the privileges has been withdrawn.

NIST Special Publication 800-12, Paragraph 10.2.1 suggests that when user accounts are no longer required, supervisors should inform application and system management so that the account can be removed in a timely manner.

In the event of compromise, the absence of a banner for WWW, FTP and/or interactive sessions may jeopardize any forms of litigation for administrative disciplinary action and civil and criminal penalties. BIA did not initially specify that ATS needed to have a log-on banner. Information received after the site visit to ATS indicated that on August 31, 2001, John Curran (BIA CIO Office) sent a copy of the BIA policy requiring notice and consent log-on banners to the TAAMS Project Manager. This in turn was forwarded to ATS.

Access should be granted only to those individuals who must use the resident information.

Recommendations: For Comments Report - Information Assurance

Impact and Importance

Deletion of user accounts is one way of preventing an unauthorized user from gaining access to an account. User accounts belonging to terminated individuals and accounts without activity for 60 or 90 days are candidates for deletion. This is especially important if the old user account had special privileges.

According to officials of the U.S. Department of Justice, legal actions against intruders have failed because the owner of computer infrastructures failed to put up the equivalent of a "No Trespassing" sign. In addition, some users complain about being monitored without having given permission to be monitored. The logon message provides an opportunity to inform users who do not consent to monitoring to log off the system.

Firewalls

Definition – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Goal – Prevent unauthorized access and protect domain information within BIANET DOI Interview Themes

EDS Observations and Findings

Three separate firewall problems were found:

- There is no firewall on the BIANET between the BIANET and the Internet Service Provider (ISP).
- There is no firewall on the ATS network between BIANET and TAAMS.
- There is no firewall on the ATS network between the ATS corporate LAN and TAAMS.

The ISP, UUNet was close to connecting a firewall to BIANET; however this effort was pre-empted by the court's Special Master, who directed that a different vendor's product to be used. The intention of the Special Master was to expedite the implementation of the firewall by recommending a known firewall vendor. If acted upon quickly, the Special Master had confidence that the other vendor could implement faster than UUNET.

This lack of protection of the BIANET affects the security of the TAAMS system because the TAAMS users connect to the ATS host for TAAMS through the BIANET. The concept of defense-in-depth or layered security is not being practiced.

The 'ATSI Dallas Network Diagram' provided during the data collection phase of this risk analysis shows no firewall between the ATS Cisco 7204 router and BIANET along the T1 frame circuit. The ATS network administrator indicated the router contained an Access Control List (ACL) that only permitted the BIANET IP addresses to pass through. This is inadequate protection of the information residing on both the Citrix server farm and the IBM AS/400 hosting TAAMS and does not implement the concept of defense-in-depth. Although authorized traffic using the connection between the TAAMS client, through the Citrix server and on to the AS/400, is encrypted both ways using Citrix proprietary

Recommendations: For Comments Report - Information Assurance

encryption, there is nothing to prevent other transmissions down the T1 frame circuit pipeline.

The 'ATSI Dallas Network Diagram' provided during the data collection phase of this risk analysis shows no firewall between the backside of the IBM AS/400 mainframe dedicated to TAAMS and other hardware on the ATS corporate LAN. The diagram does not indicate a physical disconnect/adequate isolation of the IBM AS/400 dedicated to TAAMS.

While the firewall is not a complete preventative measure to prevent attacks, the implementation of one or more firewalls will mitigate the risk to TAAMS information. The lack of firewall protection leaves many channels open to destroy or compromise the system. Firewalls insulate and protect an organization's private networks from public networks by establishing controls on the traffic allowed between them. Firewalls are relatively easy to deploy and manage. Standard industry practices for protecting government data suggest the implementation of a firewall, as is an essential element in a security strategy. NIST Special Publication 800-27, Paragraph 2.3, the *Information Assurance Technical Framework* (<http://www.iatf.net>), and the Department of Defense (<http://www.c3i.osd.mil/org/cio/gigja061600.pdf>) all advocate the use of multiple information technology protection methods or approaches to establish a composite security posture adequate to deter threats.

Impact and Importance -- High

It is understood that BIA is currently planning to have CheckPoint-1 firewalls installed on the BIANET between the BIANET and the connection to their ISP's public Internet. However, during the 'snap shot in time' of this assessment, there were no firewalls on the BIANET. Without properly configured firewalls between the BIANET and the public Internet, there can be no assurance of protection against the problems that can be introduced due to Internet access (e.g., hacking, denial of service attacks).

As there are no firewalls between the BIANET and the public Internet there is little in place to prevent an unauthorized user from getting into the BIANET. In addition, without another firewall between the BIANET and the T1 frame circuit to ATS in Dallas there is little to prevent an unauthorized user who has gained access to the BIANET (or an authorized user attempting unauthorized actions) from continuing down the communications pipeline to ATS in Dallas.

Recommendations: For Comments Report - Information Assurance

Without a physical disconnect or adequate isolation, there is the possibility of data contamination being introduced between the ATS corporate LAN and TAAMS. This is important because ATS employees working on other projects or for other clients have not been subjected to the background investigation required for employees working on the TAAMS project. ATS also has at least one foreign national working on the TAAMS project who does not have access to TAAMS but does have access to the ATS corporate LAN. Another point of interest that would suggest the need for adequate isolation from the corporate LAN is the fact that ATS is a wholly owned subsidiary of a Canadian company. One can surmise that there is email message traffic going across the corporate LAN between ATS and its parent company and it would be prudent to mitigate any chance of that traffic contaminating TAAMS data.

Auditing and Intrusion Detection

Definition – A system that monitors the network for attacks and has auditing capabilities. An audit trail produces a chronological record of system activities.

Goal – To detect attacks on the system and to enable the reconstruction and examination of the sequence of events to provide aid a security investigation.

EDS Observations and Findings

Discussions with the BIA network staff indicated that an Intrusion Detection System (IDS) was not currently installed on the BIANET. Discussions with the ATS staff indicated that although they do not have an IDS, they do use security audit tools that will alert them on their pagers in the event of network problems.

ATS has an active audit system. It notifies them when there is a hardware or software failure. It also logs appropriate information for later review. The ATS staff only uses the information on an exception basis.

Impact and Importance

Combining firewalls and IDS together is just one way to apply the concept of defense-in-depth or layered security. NIST Special Publication 800-27, Paragraph 2.3, the Information Assurance Technical Framework (<http://www.iatf.net>), and the Department of Defense (<http://www.c3i.osd.mil/org/cio/gigia061600.pdf>) all advocate the use of multiple information technology protection methods or approaches to establish a composite security posture adequate to blunt threats.

It is understood that BIA is currently planning to have a CheckPoint-1 IDS product installed on the BIANET. However, during the ‘snap shot in time’ of this assessment, there was no IDS on the BIANET. An IDS, with sensors strategically placed, is another way to protect the BIANET. Depending on the location of the sensors, email, web, and other key servers identified by management can be monitored for both incoming and/or outgoing traffic.

If ATS does not have a contractual requirement to provide IDS protection the vendor is free not to do so. Defense-in-depth is a recommended action, but not mandated to service bureaus.

ATS increases the risk of intrusion by not regularly and routinely monitoring the audit logs.

Recommendations: For Comments Report - Information Assurance

Data Integrity

Definition – Assurance that information is protected and can only be accessed or modified by those authorized to do so.

Goals – Provide accurate information to authorized users.

EDS Observations and Findings

ATS developers installed a "backdoor" that allows BIA direct access to the TAAMS database by circumventing the monitoring and auditing process. The backdoor approach breeches the data integrity protections. The "backdoor" was established at the direction of BIA by ATS in an attempt to expedite data cleanup. This was necessary because of inconsistencies in the legacy systems. A report is generated of anomalies to be cleaned up, however, there is no follow-up to monitor progress of clean up from initial data load. There has been no process identified to disable this function at a later date.

Impact and Importance

This "backdoor" poses a unique threat by potentially allowing disgruntled co-workers, ex-employees, and hackers to gain complete control and sabotage the database. This "backdoor" is a security breach in that as long as owner names are valid in the TAAMS database, transactions will not show up an anomaly in the transaction audits. While an individual may be a valid landowner, the individual may not be the valid owner of a particular piece of land. This "backdoor" could lead to a lack of accountability and potentially subjects the ATS and the Federal Government to huge dollar losses through fraudulent data.