

2008 ANNUAL SELF-GOVERNANCE CONFERENCE
20th Anniversary of Tribal Self-Governance: Celebrating Excellence
Riviera Hotel & Casino; Las Vegas, Nevada
Thursday, May 1, 2008

BREAKOUT SESSION 3:
SECURITY CLEARANCES (FEDERAL IT SYSTEMS, TRUST RECORDS)

Moderator: Stephanie Birdwell, BIA
Recorder: Ashlei Ashmore, Cherokee Nation

Panelists: Vickie Hanvey, Cherokee Nation
Lee Frazier, OST
Sanjeev Bhaguwalia, OCIO
Jackie Johnson, BIA
Nicole Jaber, OCIO

Vickie Hanvey:

DOI 2008 Negotiation Guidance:

- The guidance language differs slightly between BIA and OST.
- Applies to BOTH tribal employees and employees of tribal contactors
- Prior to being granted access to
 - A. DOI automated information technology systems and/or
 - B. trust records in any electronic data or hardcopy format
- Both require three conditions be met
 1. Must successfully complete BIA/OST trust automated technology systems training (and complete annually thereafter)
 2. Must be favorably screened and a final favorable suitability determination issued
 3. Must also successfully go through a Personal Identity Verification process
- Guidance states: Costs will be incurred by the BIA (or OST).
- Additional OST requirements
 - Take logical and physical steps necessary to secure trust information in the event of a security related incident and notify OST within 24 hours of discovery
 - Notify OST, within 24 hours, of exiting employees who no longer require systems access.
- Should a Tribe/Consortium choose not to use the Guidance language in its funding agreement a disclaimer is requested stating that none of the Tribes/Consortium's employees or employees of its contractors will have access to DOI automated information technology systems or DOI Trust records in any electronic data or hardcopy format.

Issues/Concerns:

I. **Access to DOI automated information technology systems**

I. Data entry access vs. Read-only access:

Security clearances for read-only access to database information which pertains to individual Tribal data only (the employee would not have access to other Tribes data). Nevertheless, a considerable amount of this information is available to the public through a FOIA request.

(As of SGAC meeting in November, it has now been determined that read-only access to the OSG database will be granted. However, there has been no such concession regarding other systems.)

II. Access to trust records in any electronic data or hardcopy format

1. This is being interpreted by negotiators to include any person who would have access to a trust record as broadly as to include the Principal Chief; all Realty staff; IT staff that would work on equipment; auditors; and even janitors who have access to clean the area.
2. Also, “employees and employees of its contractors” had been interpreted to include appraisal contractors engaged to conduct an appraisal on a trust property. [OST has now determined that appraisal contractors DO NOT require a background investigation.]

III. General Policy Issues

1. Applicability to Contractors (including Tribes):

To our knowledge, the Department Manual has not been updated to include information regarding tribal requirements for background investigations.

- DM 441: DOI Departmental Manual

Part 441 Section 3.11 “*Contractors. Contractors are not Federal employees and cannot hold national security positions or public trust positions. Nevertheless, contractors may be required to undergo background investigations. To that extent, further guidance will be forthcoming.*

CONTRACTOR/CONSULTANT POSITIONS (TO BE INCLUDED AT A LATER TIME)”

What is the status of updating the DM441 Policy?

2. Risk Assessments:

The requirement for background investigations (security clearances) should be based upon risk and the management of that risk. Tribes have not been apprised of the risk assessments conducted by the Department, nor if such risk assessments have been conducted for tribal “contractors”. Referred to handout.

FISMA, NIST HSPD-12 and OMB A-130 apply to all federal departments and agencies. How the individual department chooses to implement the standards is left to the department policy decision-makers. **What risk assessments have been conducted by the BIA or OST?**

3. Compliance and Processing Time:

Tribes are currently operating certain trust functions without background investigations. It has been reportedly taking six months to almost a year to process background investigations.

What is the procedure for processing background investigations especially for multiple systems with BIA and OST? Rhonda Butcher reported that her background investigation has been completed but she has no “sponsor”.

Sanjeev Bhaguwalia:

I. CIO:

- a. Chief Information Officer; has to maintain 12 (CCA96) core competencies

- i. Security and Information Assurance is one of the 12 that Mr. Bhaguwalia is responsible for as a CIO.

II. Security Clearances:

- a. Why; Federal Law and Presidential Directive
 - b. What; NACI and Credit Check
 - c. Who; Anyone who accesses any federal owned facility or system; currently 380 tribal users with access to BIA applications
 - d. Where; Personnel security module , IIS
- III. Vision for Trust
- a. Currently in front of judge to get reconnected to the internet
 - i. Internet is key component of IA OCIO Vision
 - b. Infrastructure is already in place
 - c. Security is a concern because we are a Nation under attack; Phishing, Identity theft
- IV. Security is everyone's responsibility
- 1. Predict
 - 2. Prevent
 - 3. Respond
 - 4. Detect
- V. Recap
- a. Confidentiality
 - b. Access
 - c. Communication
 - d. Dawn of new

Lee Frazier:

- I. When agencies were reviewed it was revealed that there was not a consistency; This is what has driven this process, Would like to get everyone on the same page through this process.
- II. We are trying to work on getting clarity and consistency when you are working with the agencies on your background investigations.

Sharon Garcia

- I. HSPD-12
 - a. Homeland Security Presidential Order No. 12 mandates government to investigate and identify standards to federal facilities and federal controlled information technology systems.
 - b. Physical and logical access requires a favorable adjudicated FBI fingerprint check and scheduled background investigation is required for logical access to federally controlled information systems technology.
 - c. What if a tribal user was disqualified? It is referred to the agencies superintendent; he then notifies the Chairman/Chief and/or Tribal Council for them to make the decision and act on this.
 - d. What is the function for completing the checks on these applicants? Forms are available; which can be complete for different levels of access/clearance

Q& A Discussion:

- I. DOI-Working on a document that lays out all of the information regarding Security Clearances; this will be available.
- II. Business Week Article , Espionage (referenced) regarding new concerns on security
- III. As a SG coordinator do I have authority to request that a Security Clearance? It is believed that Yes a SG coordinator would have authority; DOI representatives are going to request that Sharee Freeman send information out to Tribes for clarification
- IV. Real ID's? Requirement to have a government issued ID to access Federal facilities etc.? DOI currently do not issue ID cards, because we hare in the process of following through on HSPD 12.
 - a. DOI is still doing this in steps...
- V. DOI request Tribal Representation; How would the Tribes like to proceed on this???
 - a. Suggested that this be addressed at General Session Review...
- VI. DOI- Once you get the access worked out, you could have access to other functions etc. This would be another benefit that this could address in the future.
- VII. The need for background checks for Youth Sensitive positions may need to be looked at. Also a more thorough look within the department (an in-depth study) would be beneficial.

Security Clearances (Federal IT Systems, Trust Records)

Handout: Vickie Hanvey

Applicable References:

- There is no applicable law referenced in the guidance, therefore the 2008 guidance requirements for DOI security clearances appear to be based upon Department policy decisions. However, there are references in other documents to FISMA.
- **FISMA:** Federal Information Security Management Act of 2002 (44USC 3542 (2)(A) Requirements for national security systems.
- **NIST:** National Institute of Standards and Technology (NIST). Sets the national standard for information technology and security.
- **HSPD12:** Homeland Security Presidential Directive 12; A one page document outlining policy for a common identification standard for federal employees and contractors.
- **OMB Circular No. A-130:** This circular established policy for the management of federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.
- **DM 441:** DOI Departmental Manual; Part 441 Personnel Security and Suitability Requirements. This part establishes the policies, regulations, and procedural guidelines for the operation of the personnel security and suitability program of the Department. This part is the controlling instruction for implementation and maintenance of the Departments personnel security program. Personnel security provisions incorporated in other Departmental directives must comply with this regulation.
- **PIV Policy and Guide:** This guidance provides policies and procedures governing the Personal Identity Verification (PIV) process and Smartcard (DOI ID Badge) issuance requirements.

Affected IT systems (includes but is not limited to):

OSG Database: Maintains financial data for all Self Governance Tribes; including the annual reprogramming request; payments, ATO and amendment history.

IRR Financial Database: Maintains financial historical data for Roads projects.

RIFDS: Road Inventory Field Data System; a new IRR inventory system recently developed to allow data entry of roads inventory at the Tribal level as opposed to bottleneck at the Regional level.

TAAMS: Trust Asset and Accounting Management System

ITARS: Indian Trust Appraisal Request Tracking System

TFAS: Trust Fund Accounting System

General Policy Issues

4. Applicability to Contractors (including Tribes):

To our knowledge, the Department Manual has not been updated to include information regarding tribal requirements for background investigations.

- DM 441: DOI Departmental Manual

Part 441 Section 3.11 “*Contractors. Contractors are not Federal employees and cannot hold national security positions or public trust positions. Nevertheless, contractors may be required to undergo background investigations. To that extent, further guidance will be forthcoming.*

CONTRACTOR/CONSULTANT POSITIONS (TO BE INCLUDED AT A LATER TIME)”

What is the status of updating the DM441 Policy?

5. Risk Assessments:

The requirement for background investigations (security clearances) should be based upon risk and the management of that risk. Tribes have not been apprised of the risk assessments conducted by the Department, nor if such risk assessments have been conducted for tribal “contractors”.

FISMA, NIST HSPD-12 and OMB A-130 apply to all federal departments and agencies. How the individual department chooses to implement the standards is left to the department policy decision-makers. **What risk assessments have been conducted by the BIA or OST?**

- OMB Memorandum M-05-24, Implementing Guidance for HSPD-12:
 - “1. To whom does the Directive apply?”
 - C. Contractor- Individual under contract to a department or agency, requiring routine access to federally controlled facilities and/or federally controlled information systems to whom you would issue Federal agency identity credentials, consistent with your existing security policies. Does not apply to: Individuals under contract to a department or agency, requiring only intermittent access to federally controlled facilities.”
 - E. Federally Controlled Information Systems- “...Applicability for access to Federal systems from a non-Federally controlled facility (e.g. researchers’ up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on the risk determination required by existing National Institute of Standards and Technology (NIST) guidance.”
- OMB A-130 Appendix III B Descriptive Information, states ““Adequate security” is defined as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.” This definition explicitly emphasizes the risk based policy for cost-effective security established by Computer Security Act.”
- Must also successfully go through a Personal Identity Verification process. This requirement is based upon PIV Policy and Guide, which states in Section 1.3 Applicability
...the standard “is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for ‘national security systems’ as defined by 44U.S.C. 3542(b)(2). ...DOI reserves the right to subject any individual to the PIV-I process following a risk-based assessment.”
Also Appendix G (3)(c) Federally Controlled Information Systems states; “Federally controlled facility (e.g. researchers’ up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on risk.”