

## Annual Tribal Trust Evaluation System Security FAQs

- 1) **Question:** Will the information in the Annual Tribal Trust Evaluation System (ATTES) be protected?

**Answer:** Yes, the ATTES information will be protected through a series of different measures to ensure the security of information within the system. These include the use of roles in the application, the use of secure communications protocols across the internet, as well as encryption and secure storage of uploaded information.

- 2) **Question:** What do you mean roles in the application?

**Answer:** Each user within the ATTES application is assigned a role which will define what areas (and information) they will be allowed to access in the system. For example, specific auditors will be assigned to specific tribes and only be able to review information for those tribes and not others. In addition, tribal members will only be able to see their tribe's information. Furthermore for tribal members, a tribal coordinator will assign the tribal member roles for their tribe which can further limit access for specific tribal members. For example, John as Tribal Coordinator may assign Carl to the Mining and Forestry areas of the overall tribal assessment. This means that Carl will only have access to those assessment questions and information.

- 3) **Question:** How will the information be protected when it is transmitted across the internet (e.g. secure communication protocols)?

**Answer:** There are two basic methods (protocols) that will be used to ensure that information transmission across the internet is secure. These are the use of SAML (Security Markup Language) tokens and SSL (Secure Socket Layer) transmission.

SAML will be used for the Authentication and Authorization of users and their roles. When the user is setup in ATTES for the first time the Identity Server is configured with the user identity and roles (see question #1). Each time a user logs into ATTES it will ask the Identity Server to authenticate the user and pass back all roles for that user in a SAML token. The token follows the user around in ATTES and the user permissions are validated with each browser request. This ensures that each browser selection is verified as correct for the roles the user has been assigned.

SSL involves the use of certificates that regulates the communication between the browser and the server(s) in the DOI Cloud Hosting Center. The certificates are used to identify a user/browser session is authorized. Once authorized the SSL and associated Certificate Manager will encrypt all communication between the user browser and the DOI Cloud hosting server, including the downloaded files. If you have used Amazon for purchasing anything, the same technology will be used in encrypting the ATTES communication as is used when you provide your credit card information to Amazon (AWS – Amazon Web Services).

- 4) **Question:** What does encryption mean?

**Answer:** Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. An encrypted file will appear scrambled to anyone who tries to view it. It must be decrypted in order to be recognized.

There are many different types of encryption algorithms, but some of the most common ones include AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish, RSA, and DSA (Digital Signature Algorithm). While most encryption methods are sufficient for securing your personal data, if security is extremely important, it is best to use a modern algorithm like AES with 256-bit encryption.

5) **Question:** Once I have sent the information, where is it stored?

**Answer:** The ATTES physical assets (hardware, etc.) will reside in one of the DOI's Cloud Hosting Centers. The Centers are secure facilities with physical access controls restricting access to the Center in general as well as areas within the Center.

6) **Question:** How is the uploaded data stored once it is transmitted? Is it stored securely?

**Answer:** The uploaded information will be stored on a secure/encrypted storage device within the DOI Cloud Hosting Center. The encryption on the physical storage device is of the same nature as is described in the answer to question #4. ATTES has added this extra layer of protection to the uploaded information as this is where the most sensitive data will reside.

7) **Question:** Will the ATTES system be compliant with Federal Government security regulations and guidance?

**Answer:** The ATTES system will be compliant with all relevant Federal Government security regulations and guidance. Of particular note are:

- FEDRAMP compliance
- FISMA certification and rating

The Federal Risk and Authorization Program (FEDRAMP) is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

FEDRAMP was created to support the government's cloud computing plan. The program is intended to facilitate the adoption of cloud computing services among federal agencies by providing cloud service providers (CSPs) with a single accreditation that could be used by all agencies. The goal of FEDRAMP is to reduce the time and money that individual agencies would otherwise have to spend on assessing a cloud provider's security. Certifications are based on a unified risk management process that includes security requirements agreed upon by the federal departments and agencies. The ATTES will be hosted inside of one of the DOI's FEDRAMP certified Cloud Hosting Environments.

The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the

Electronic Government Act of 2002. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner. The National Institute of Standards and Technology ( NIST ) outlines nine steps toward compliance with FISMA:

1. Categorize the information to be protected.
2. Select minimum baseline controls.
3. Refine controls using a risk assessment procedure.
4. Document the controls in the system security plan.
5. Implement security controls in appropriate information systems.
6. Assess the effectiveness of the security controls once they have been implemented.
7. Determine agency-level risk to the mission or business case.
8. Authorize the information system for processing.
9. Monitor the security controls on a continuous basis.

The ITRS system will have a FISMA moderate rating.

8) **Question:** What does Section 508 compliance mean?

**Answer:** Section 508, an amendment to the United States Workforce Rehabilitation Act of 1973, is a federal law mandating that all electronic and information technology developed, procured, maintained, or used by the federal government be accessible to people with disabilities. Technology is deemed to be "accessible" if it can be used as effectively by people with disabilities as by those without. To demonstrate that a product or Web service is in compliance with Section 508, the creator completes a Voluntary Product Accessibility Template (VPAT), an "informational tool" that describes exactly how the product or service does or does not meet Section 508 standards. The completed VPAT gets posted on the creator's Web site to provide government officials and consumers with access to the information.