FISSEA Security Awareness, Training, & Education Contest

Entry Form

Please review rules before completing entry form including the due date. No late entries will be accepted. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Ruth Petersen for the NASA IT Security Awareness and Training Center Team (ITSATC)

Organization: NASA ITSATC

Type of Entry: Role-Based Training & Education

Title of Entry: Lesson 2 Managing Laws and Regulations, *Information Security for Chief Information Officers – Intermediate*

Description of Entry:
The NASA IT Security Awareness and Training Center (ITSATC) is currently developing role-based training in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. The NIST SP 800-16 recommends 46 modular components for building role-based training, with specifics for each role. The goal of the NASA ITSATC is to develop a role-based training course for every Agency role with significant security responsibility at a beginning, intermediate, and advanced level (as per the NIST SP 800-16). The ITSATC has completed 39 beginning and 23 intermediate modules. We currently offer the following courses at the beginning level:

- Certification Agents & Authorizing Officials (CA&AO)
- Chief Information Officers
- Organizational Computer Security Officials (or ISSOs)
- System Administrators
- System Owners (under revision as Information System Owners/Information Owners)

And we offer two courses at the intermediate level:

- Chief Information Officers
- System Administrators

Our training incorporates information from the other NIST SP publications that support FISMA, as well as other laws and NASA-specific information. Our courses are 508 and Shared Content Object Reference Model (SCORM) compliant, Learning Management System (LMS) compatible (i.e., tracking requirements), and operable in a Federal Desktop Core Configuration (FDCC) environment. As ISS LOB T2T providers, we have shared these role-based courses with 15-20 government agencies via CD at no charge. We routinely revise the courses based on feedback and updates in Federal and NASA guidelines/publications.

Chief Information Officers (CIOs) are the heart of NASA's Information Security Program. The intermediate course was created to help CIOs and their staff better protect the information, information systems, and security programs they are responsible for. The course is available on SATERN (System for Administration, Training, and Educational Resources for NASA) to all NASA employees.

According to the NIST SP 800-16, managers should be able to **understand applicable governing documents and their interrelationships and interpret and apply them to their area(s) of responsibility**. Lesson 2, Managing Laws and Regulations, discusses the development of policies that reflect the legislative intent of applicable laws and regulations, including Federal Government-wide and NASA-published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of Information Technology (IT) resources.

The objectives of Lesson 2 are to educate CIOs to better:

- Analyze the impact of information security laws and regulations applicable to their areas of responsibility.
- Determine how applicable laws and regulations affect their areas of responsibility and interact with organizational goals and existing policy.
- Apply mandated requirements and standards in the form of appropriate policies to their areas of responsibility.

Lesson 2 introduces the fundamental concepts needed to understand the subject and gives examples and practical exercises to reinforce, apply, and extend the learning. From each screen, learners can access a glossary, a list of acronyms, course URLs, a link for help with questions, the course map, and a text-only version. Screens can be printed. And if learners are interrupted and unable to complete a lesson at one sitting, they can set a bookmark and return to that screen at a later time. The conclusion provides a summary of the most important topics introduced in the lesson.

FISSEA Contest 2010

Name:	**Ruth Petersen for the NASA IT Security Awareness and Training Center Team (ITSATC)**
Organization:	**NASA ITSATC**
Type of Entry:	**Role-Based Training & Education**
Title of Entry:	**Lesson 2 - Managing Laws and Regulations, *Information Security for Chief Information Officers – Intermediate***

Description of Entry

Chief Information Officers (CIOs) are the heart of NASA's Information Security Program. The intermediate course was created to help CIOs and their staff better protect the information, information systems, and security programs they are responsible for. The course is available on **SATERN** (System for Administration, Training, and Educational Resources for NASA) to all NASA employees.

According to the NIST SP 800-16, managers should be able to **understand applicable governing documents and their interrelationships and interpret and apply them to their area(s) of responsibility**. Lesson 2, Managing Laws and Regulations, discusses the development of policies that reflect the legislative intent of applicable laws and regulations, including Federal Government-wide and NASA-published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of Information Technology (IT) resources.

The objectives of Lesson 2 are to educate CIOs to better:

- ❖ Analyze the impact of information security laws and regulations applicable to their areas of responsibility.
- ❖ Determine how applicable laws and regulations interact with organizational goals and existing policy.
- ❖ Apply mandated requirements and standards in the form of appropriate policies to their areas of responsibility.

Lesson 2, Managing Laws and Regulations, introduces the fundamental concepts needed to understand the subject and gives examples and practical exercises to reinforce, apply, and extend the learning. From each screen, learners can access a glossary, a list of acronyms, course URLs, a link for help with questions, the course map, and a text-only version. Screens can be printed. And if learners are interrupted and unable to complete a lesson at one sitting, they can set a bookmark and return to that screen at a later time. The conclusion provides a summary of the most important topics introduced in the lesson.

Screen 2 of 15 – Lesson References

Each lesson contains a list of Federal and NASA documents used as references. Links within the course open in a new page and provide a definition, additional information, or an applicable web page.

Screen 3 of 15- Analyzing the Impact of Information Security Laws and Regulations

Notes provide helpful additional information.

Screen 4 of 15 – Exercise for Application

Practical exercises reinforce, apply, and extend the learning and provide immediate, positive feedback.

Exercise for Application:

Information security laws and regulations mandate that information security be part of the entire System Development Life Cycle (SDLC) and not just an afterthought to building a system. How can this impact NASA's Information Security Program?

- A — Eliminates the need to establish and maintain a unifying vision and strategic direction.
- B — Eliminates the need for developing additional security controls to supplement the controls already in place.
- C — Reduces the risk that any changes made to a system result in a compromise to system or data confidentiality, integrity, or availability.
- D — Eliminates the need for modifying selected controls that are deemed to be less than effective.

That's Right!

C is the correct answer.

Screen 5 of 15 - Understanding the Effect of Laws and Regulations on NASA Policy

Examples given to clarify or explain information further are listed with the "e.g." icon.

Understanding the Effect of Laws and Regulations on NASA Policy

There are laws affecting the security of information systems in general. And each particular system might have specific guidelines. Review NASA policies and guidelines [NASA Policy Directives (NPDs), NPRs, and Standard Operating Procedures (SOPs)] to find the laws and regulations that apply to your specific programs or systems. NASA policies and guidelines can be accessed via NASA Online Directive Information System (NODIS). SOPs can be accessed through NODIS under *Other Policy Documents*. The list of SOPs constantly changes because of expiration, revision, or incorporation of the SOPs into NASA Interim Technical Requirements (NITRs).

FISMA requires security planning by all Federal agencies, and NIST provides documents to aid Federal agencies in security planning. The use of security controls from **NIST SP 800-53** and the incorporation of baseline controls as a starting point in the control selection process facilitate a more consistent level of security in NASA's information system. The use of security controls from NIST SP 800-53, also allows for flexibility in tailoring the controls based on specific organizational policy and requirements documents.

NPR 2810.1 includes information on NASA-specific areas of compliance with existing laws and policies. The obligation to measure performance and reduce cost is driven by Federal regulatory and NASA requirements. These measurements are designed to provide substantive justification for decision making based on NASA's goals and objectives. And they should measure the effectiveness of the Information Security Program, policies, and requirements.

e.g. One such area is restriction of the distribution of information. NPR 2810.1 provides a table that lists information appropriate for publication on the Internet. All NASA information and data made available to the public at large via the Internet, unless protected by appropriate access controls, are considered published and subject to the requirements of NPR 2810.1.

Screen 8 of 15 - Sensitive But Unclassified Information

This screen provides examples of Center policies for handling SBU information.

Managing Laws and Regulations Training Module - Windows Internet Explorer

https://satern.nasa.gov/customcontent/scorm/ITS-RB2-CIO/lesson02/index.html

Sensitive But Unclassified Information

NASA's current policy for identifying and safeguarding Sensitive But Unclassified (SBU) information states that when transmitting e-mail messages outside the Agency's secure network (nasa.gov), you should encrypt e-mail messages and attachments that contain SBU information. If you feel that your Center needs a stronger policy to better protect SBU information, you should develop and enforce that policy for your Center.

e.g. Your policy might state that NASA employees must encrypt SBU information that should not be made publicly available while in transit and "at rest."

e.g. One Center's procedural requirements state:
"SBU information shall be safeguarded as follows:

a. Attended when in use.
b. Access limited to those with "need-to-know."
c. Limit number of hard copies.
d. Stored under lock and key when unattended (locked desk, locked office, locked cabinet, or locked office suite).
e. SBU cover sheet (NASA Form 1686, *Sensitive But Unclassified*) when transmitted on or off Center (optional for FAR, FOUO, Export Control, FOIA, but physical protection is the same as for SBU).
f. Stored on secure server with appropriate markings/warnings (contact the CIO to see what your secure server is).
g. No further dissemination of SBU without approval.
h. **Encrypted e-mail transmission.**
i. Transmitted by Secure Fax or person to person tracking on unclassified fax.
j. Destroy by shredding, burning, and removing from computer systems.

Individuals shall be subject to administrative sanctions if they disclose information designated SBU or violate NASA SBU policy. Sanctions include, but are not limited to, a warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, or discharge."

Screen 9 of 15 - Gaining Access to NASA Information and Information Systems

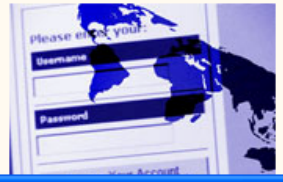
Links within the course open in a new page and provide a definition, additional information, or an applicable web page. Items shown in **a bolded blue color** provide additional rollover information.

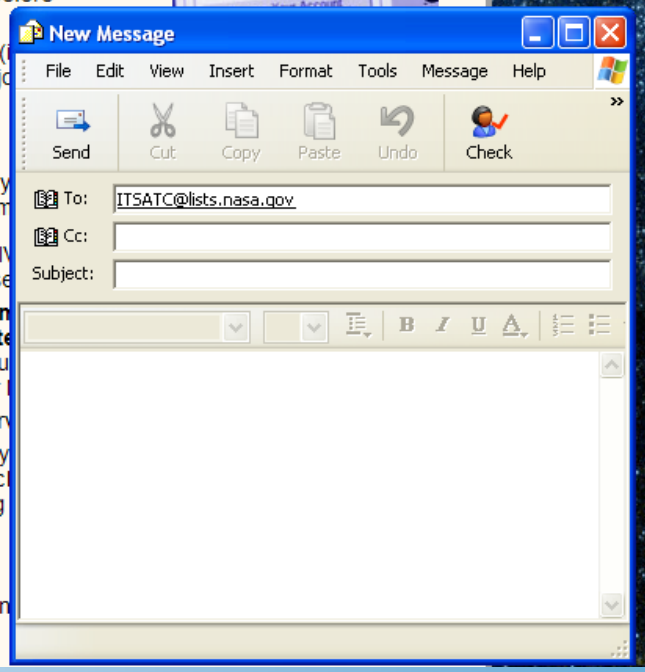
Gaining Access to NASA Information and Information Systems

The OMB and NIST documents listed below require that individuals be properly trained in how to fulfill their security responsibilities before giving them access to or continuing access to Agency information systems:

- OMB Circular A-130, Appendix III, states, "*Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall ensure that employees are versed in the rules of the system . . . and apprise them about available technical assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.*"
- OMB Memorandum 07-16 states that agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems.
- **NIST SP 800-50** states that managers should ensure that all users (i contractors) of the systems and majo applications) are a lfill their security responsibilities be

Building an Information Technology Security Awareness and Training Program





You might, therefore, decide to develop and enforce a stronger policy for y the new hire process to enable faster access to Agency information system

- New employees may work with their Personal Identity Verification (PI to their start date to get a head start on the new employee's ODIN se
- **As part of the new employee's first-day orientation, all new em *Security for New Employees* training CD, which is an abbreviate** New employees have 30 days to complete required information secu System for Administration, Training, and Educational Resources for
  - A SATERN account is automatically created for NASA civil serv
  - Support service contractors may create their own accounts by home page as soon as they have an e-mail account. The Tec Technical Representative (COTR) is responsible for ensuring information security training.

The *Introduction to IT Security for New Employees* train IT Security Awareness and Training Center (ITSATC).

Screen 13 of 15 - Security Authorization (SA)

Security authorization information is based on the latest revision of the NIST SP 800-53.

Managing Laws and Regulations Training Module - Windows Internet Explorer

https://satern.nasa.gov/customcontent/scorm/ITS-RB2-CIO/lesson02/index.html

Security Authorization (SA)

Security authorization is part of a dynamic, risk management process. You have the following responsibilities in relation to security authorization for information systems:

- Encourage cost-effective practices such as maximum reuse and sharing of security-related information to include:
  - Threat and vulnerability assessments,
  - Risk assessments,
  - Results from common security control assessments, and
  - Any other general information that may be of assistance to **Information Security Officers** and their supporting security staffs.
- In concert with the AO, determine appropriate allocation of resources for information security programs and systems.
- In certain instances, operate as the AO for Agency-wide General Support Systems (GSS) or as co-AO with other senior officials for selected Agency systems.

NIST SP 800-37, *Guide for the Security Certifications and Accreditation of Federal Information Systems*, is in the process of being revised. Its new title will be: *Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach*. It is important that you as CIO understand the impact that revisions in this Guide have on the authorization process and make adjustments in Center policy as needed.

The NIST SP 800-37 is being revised to:

1. Develop a common SA process for Federal information systems (currently known as the certification and accreditation process).
2. Express the process of authorizing information systems to operate as an integral part of the System Development Life Cycle (SDLC) and the Risk Management Framework (RMF).
3. Provide a well-defined and comprehensive SA process that helps ensure appropriate entities are assigned responsibility and are accountable for managing information system-related security risks.
4. Incorporate a risk executive (function) into the SA process to help ensure that managing security risks from individual information systems: (a) is consistent across the organization; (b) reflects organizational risk tolerance; and (c) is performed as part of an organization-wide process that considers other organizational risks affecting mission/business success.

Internet 100%

Sample Exam Question

After obtaining exam results, learners are able to review the questions to learn which questions they missed and the correct answers to those questions.