

INFORMATION TECHNOLOGY SERVICES



NIST 800-171 COMPLIANCE AT FSU - CONTROLLED UNCLASSIFIED INFORMATION

THE
FLORIDA STATE
UNIVERSITY



WHAT IS NIST 800-171 COMPLIANCE AND WHY DO WE HAVE TO DO IT?

- Any Controlled Unclassified Information (CUI) residing in nonfederal information systems and organizations must be protected following the control requirements of NIST 800-171.
- FSU has research projects which have been identified as having CUI data.
- FSU agreed to protect this data and meet the required controls when these contracts and grants were accepted by the University.
- FSU Research along with ITS is working to ensure that each project or contract which requires compliance, meets that compliance.
- If we were to get audited, FSU Research must be able to show that we are meeting with our compliance requirements.
- By developing a standard compliance methodology for all FSU research requiring compliance, it is hoped that researchers will be able to dedicate their time on research and not have to dedicate as much time on meeting the requirements of the controls.
- FSU Research also sees compliance as a possible competitive advantage for FSU researchers when competing with other Universities which cannot meet these compliance requirements.



WHAT IS CONTROLLED UNCLASSIFIED INFORMATION?

Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

-- Executive Order 13556



WHY ARE WE SEEING THESE RULES?

The protection of **Controlled Unclassified Information** while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can *directly* impact the ability of the federal government to successfully carry out its designated missions and business operations.

-- NIST Special Publication 800-171





HOW TO IDENTIFY CUI

- CUI Supports federal missions and business functions that affect the economic and national security interests of the United States.
- Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation or governmentwide policy may be designated as CUI.
- The federal organization is responsible for informing the nonfederal organization:
 - DFAR (DoD contracts)
 - Requires that CUI be marked
 - Sub-contractors dependent on the prime may not receive the same information provided to the prime.
 - FAR (Civilian agency contracts)
 - FAR Rule requires civilian agencies to mark CUI
 - A CUI notice will be issued notifying agencies to identify CUI in contracts and agreements.
- If it is not clear, the nonfederal organization should ASK the federal organization.
- FSU often identifies a contract or grant as having CUI by the inclusion of the following clauses within the contract:
 - FAR Clauses 52.204-2, 52.204-21, and any others that may require compliance.
 - DFARS Clauses 252.204-7008, 252.204-7009, 252.204-7012 and any others that may require compliance.



WHAT IS NIST 800-171?

- NIST Special Publication 800-171 defines the security requirements (controls) required to protect CUI in nonfederal information systems and organizations.
- Information systems that process, store, or transmit CUI may be *federal* or *nonfederal*
 - When *federal* (including contractors operating *on behalf of*), agency security requirements are applied (i.e., FISMA/RMF)
 - When *nonfederal*, SP 800-171 security requirements are applied (FSU is a non-federal organization)



HOW DOES FSU PLAN ON MEETING THE CONTROL REQUIREMENTS?

- Utilizing a standard model, FSU employs cloud based services (currently Amazon Web Services) in addition to standardized policies and procedures to meet the control requirements.
- This model provides the flexibility to meet research data security needs whether entirely cloud based or in a hybrid model with on premise resources.



CAN'T RESEARCHERS JUST DO THIS THEMSELVES?

- In order to ensure that control requirements are being met, Research has decided a centrally managed solution is the most cost effective and manageable way to meet the controls.
- Most research units do not have the resources available to meet all 110 of the controls independently.




WHAT CAN I DO TO HELP ENSURE WE MEET THE COMPLIANCE REQUIREMENTS?

- Work with Research and ITS/ISPO to ensure that CUI data is identified and protected appropriately.
- As you solicit new grants and contracts, cooperate with the designated staff to ensure any CUI data is protected appropriately.
- Register for and complete the training detailed on the SANS SECURE THE HUMAN TRAINING slide later in this presentation.
- Promptly notify ISPO if you suspect that any CUI data has been compromised (lost, stolen or suspected to have been inadvertently divulged).



WHAT DO I DO IF I NEED HELP

- Please follow the Incident Response Procedures for details on how open a support ticket. These can be found here:
- Note that Security Incidents need to be reported within 72 hours of discovery. Please follow the Incident response procedures if a Security Incident is discovered or suspected.
- The basic steps for opening a support ticket are to:
 - Contact your local IT support first to determine if your issue can be resolved locally
 -  If it cannot be resolve locally, open a ticket in the ITS Service Center or call 644-HELP.
 - When you create the case, at a minimum, enter:
 - Provider Group – ITS-NIST
 - Category – IT Support Services
 - Specialty Type – NIST
 - As much detail regarding your issue as possible.
- Your case will then be directed to the appropriate staff.



TRAINING

- Control family 3.2 is Awareness and Training. It consists of three controls detailing the requirements to ensure that FSU personnel are made aware of the security risks associated with their activities and that they are aware of the applicable FSU policies and procedures.
- In order to make the best use of your time, we have broken the training into two parts.
 - This PowerPoint presentation.
 - The SANS Securing the Human online training.
- This Security Awareness training has been customized with modules that meet the NIST 800-171 requirements.
- This training can be taken at your leisure as long as it is completed by the timeframe requested by ITS/ISPO. This makes the best use of your time by not requiring you to schedule time to attend an on site presentation.
- Access to the CUI data will be restricted to those users who have completed the training (this is a requirement of NIST 800-171).
- Reports will be used to identify staff who have met these training requirements.



FSU POLICY

- FSU has very detailed Information Security and Information Privacy Policies. These can be found here:
- Information Security Policy:
<http://policies.vpfa.fsu.edu/policies-and-procedures/technology/information-security-policy>
- Information Privacy Policy:
<http://policies.vpfa.fsu.edu/policies-and-procedures/technology/information-privacy-policy>
- All FSU employees should be familiar with these policies.



SANS SECURE THE HUMAN TRAINING

- Please register for and attend the Security Awareness training
- To register, go to: <https://bit.ly/2lyqS8D>
- After registering, you will be approved for the training by the FSU ISPO training coordinator. This can take up to one day, however he usually responds within an hour or so of receiving your registration request.
- To access the training after you have registered, go to: <https://vle.securingthehuman.org/auth/login.php>
- When requested to Select the Course you wish to take, please select CUI:

A screenshot of a web registration form titled "Register for Security Awareness Training". The form has a light green background. It contains several input fields: "First Name" with the value "Fred", "Last Name" with "Flintstone", "Email Address" with "fflintstone@fsu.edu", and "Date" with "5/10/2018". There are two dropdown menus: "Primary Role" set to "Employee" and "Select Course" set to "CUI". The "Select Course" dropdown is circled in blue. Below the form, there is a checkbox for "I give permission to Florida State University to release my name and email address to SANS Institute who is responsible for providing the training videos." and a button labeled "More about the courses".

Register for Security Awareness Training

Date

First Name Email Address

Last Name Primary Role

Select Course

Please select a course that seems best suited to you. You're welcome to take any or all courses on this site as long as you register for one course at a time.

I give permission to Florida State University to release my name and email address to SANS Institute who is responsible for providing the training videos.



CONTACTS

Mike Boll

Research Data Security Specialist

(850) 645-3602

mboll@fsu.edu

Diana Key, Director

Research Compliance Programs

(850) 644-8648

dkey@fsu.edu