CUI / CDI
NIST SP 800-171
Onboarding

Initial information for Principal Investigators working with data requiring NIST SP 800-171 controls

Updated: October 12, 2017

Questions can be submitted to:
cui-support@list.arizona.edu
Outline

1. What is CUI / CDI / NIST SP 800-171?
2. “Green” versus “Red” machines
3. AWS GovCloud Environment Overview
4. GovCloud S3 Bucket Application
5. CUI “Green” Laptop
6. Continuous Monitoring Overview
**What is CUI / CDI / NIST 800-171?**

**Controlled Unclassified Information (CUI)**
Executive branch data designation for data requiring safeguarding and dissemination controls to protect the ability of the federal government to successfully carry out its designated missions and business operations.

**Covered Defense Information (CDI)**
Data that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of a DoD contract. DFARS 252.204-7012 promulgates CDI as CUI.

**NIST SP 800-171**
Defines 109 security controls for protecting the confidentiality of CUI. These controls are mapped to the medium set of NIST 800-53 confidentiality controls.
“Green” versus “Red” machines

Green Machines

- An asset that can **locally** store, process, or transmit CUI, or provide security protection for such components
- Green machines are managed assets that are in-scope for all 109 controls in the NIST SP 800-171.

Red Machines

- An asset that **does not** locally store, process, or transmit CUI, or provide security protection for such components
- Red machines are unmanaged assets that may access the GovCloud environment by going through a terminal host.
Amazon Web Services GovCloud

• Amazon Web Services (AWS) offers reliable and scalable cloud RAM/CPU services

• The GovCloud region of AWS offers NIST SP 800-171 compliant security of the cloud
  – UA is still responsible for NIST SP 800-171 compliance in the cloud

AWS GovCloud Compute Environment

• Linux or Windows

• Custom storage / RAM / CPU / application installations

• Can be turned off when not being used (to save RAM / CPU costs)
Amazon Simple Storage Service (S3)
- Amazon S3 stores data as objects within resources called “buckets”
- We have configured our S3 buckets to encrypt data at rest according to FIPS 140-2, Level 2, requirements

S3 Bucket “Drop Box” Application
- UA developed application that sits on top of S3 bucket that allows a project sponsor to connect and retrieve data via two-factor authentication
  - Sponsor is required to have a Net ID, which is created as part of a Designated Campus Colleague (DCC) request using the specialized “Sponsored Research Authentication” (SRA) subtype
    - SRA DCC accounts can be requested by departments after following all applicable Export Control processes
CUI “Green” Laptop

- Capable of locally storing, processing, and transmitting CUI data
- In-scope for all 109 controls of the NIST SP 800-171
- To be used for CUI work only
- USB ports should not be utilized unless the device is specifically authorized by the project Technology Control Plan (TCP)
- Runs Windows 10 with NIST SP 800-171 required security hardening
- Requested through departmental IT Staff
Continuous Monitoring

Requirements

• All assets that store, process, or transmit CUI data, or provide security for such components are required to be continuously monitored for security incidents
  • There is a required 72 hour reporting window for reporting cyber incidents

Current Configuration

• All assets have Splunk agents send logs to a central aggregator in the AWS GovCloud environment
• Logs are continuously monitored by an external Security Operations Center (SOC)
  • Alerts are escalated to the UA Operations team