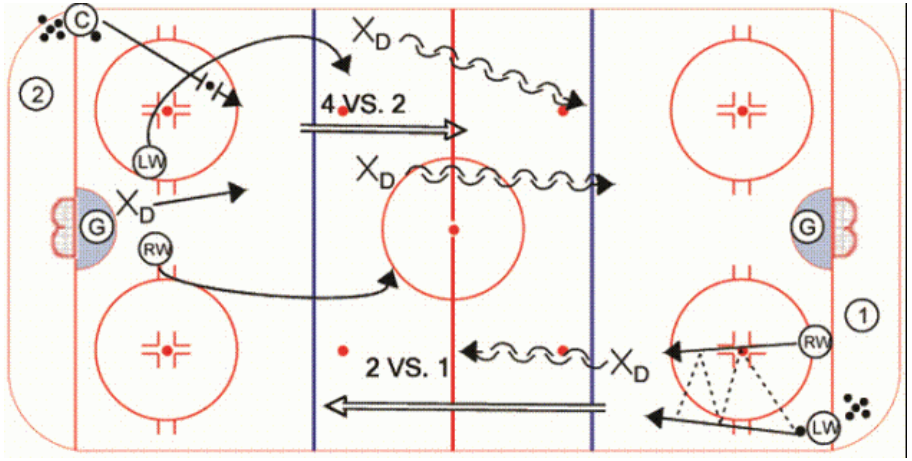
PennState
Applied Research Laboratory

Pennsylvania State University
Applied Research Laboratory

Creating a Strategy in SSP Preparation

Andrew G. Spragg

- How do you mix security and innovation?
- How do you make your approach repeatable?



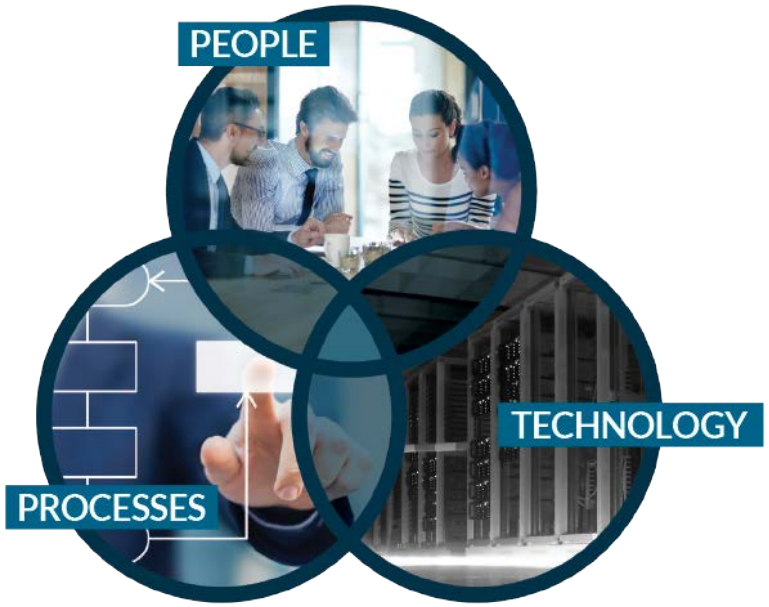
"The game plan might be different based on the opponent, but the approach is the same." *Andre Ware*

Determining Requirements

- Sponsor/Authorizing Official Expectations
- Compliance Outcome
- System Type
- SSP Approach

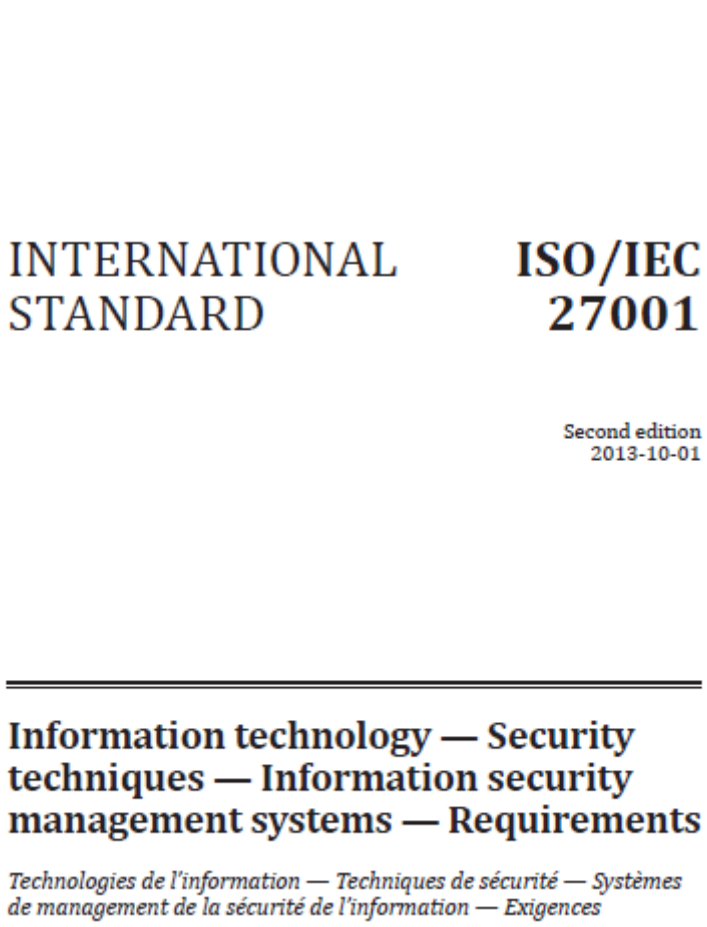
Sponsor Requirements

- Sponsor
  - Technical Knowledge
  - Risk/Compliance Approach
- Audit Authority
  - Government
  - Third Party
  - Self
- Budget
  - Hardware
  - Software
  - Personnel



Compliance Outcome

- Standards/Frameworks
  - NIST
  - ISO
  - CIS
  - HIPAA
  - SOX
  - PCI-DSS
- Compliance
  - Requirement
  - Guideline



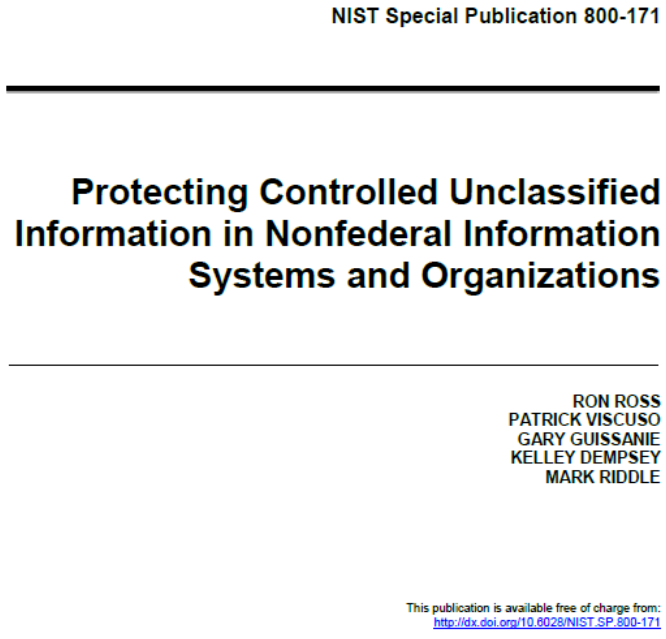
INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences



NIST Special Publication 800-171

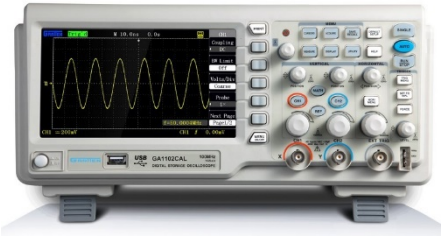
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

System Types

- Type:
  - Research equipment
    - Electrical (Safety/Quality)
    - Medical
    - Signal (Wave Form Generator)
    - Computer Numerical Control (CNC Mill)
  - Specialized compute systems
    - GPU
    - CPU
  - Networked systems
    - Corporate (Administrative)
    - Research



SSP Approach

- Single Document
  - Provides technical data on each control
    - Perceived in the weeds
  - Large document
    - Each control
- Multiple Individual Documents
  - Large amount of overhead resources
  - Specialized answers for each system
- Master System Security Plan
  - Overarching security approach
    - Covers Common Controls
  - Individual System Plans
    - Covers the Deltas

3: REQUIREMENTS

3.1: ACCESS CONTROL

3.1.1 <Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).>

3.1.2 <Limit system access to the types of transactions and functions that authorized users are permitted to execute.>

3.1.3 <Control the flow of CUI in accordance with approved authorizations.>

3.1.4 <Separate the duties of individuals to reduce the risk of malevolent activity without collusion.>

3.1.5 <Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 <Use non-privileged accounts or roles when accessing nonsecurity functions.>

3.1.7 <Prevent non-privileged users from executing privileged functions and audit the execution of such functions.>

Requirement	SP 800-171r1 Requirement [and guidance]	ARL Requirement Clarification/Elaboration	ARL Implementation Guidance	Example High-level plan for implementation
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).	This requirement only deals with initial system access. The actions taken after this initial access are addressed by other requirements such as 3.1.2. Related requirements: 3.1.2, 3.1.5, 3.1.7.	None	**Example:** System accounts are created only for individuals approved to have access and account access requires identification and authentication to ensure that only the authorized user is accessing that account. **Example (isolated system):** Taking advantage of being an isolated system, system access is limited to only authorized users by physical access control that restricts unescorted physical access to only authorized system users. In addition, for components having user login capability, user identifier and password are required as part of login to enable control in requirements 3.1.2 of user actions after login.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	In addition to enforcing access to the system, you must also define and enforce authorizations as to what actions users are allowed to perform after having gained system access (e.g. hierarchy for user accounts, not having admin/root privileges on all user accounts). Related requirements: 3.1.1, 3.1.5, 3.1.7.	None	**Example:** Permissions applied to user accounts reflect the defined user access authorizations and the access enforcement mechanisms included within the components of the system enforce access according to these permissions.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	"The flow of CUI" refers to data in transit. This includes CUI to/from removable media. By controlling flow of CUI, the system gains the ability to have finer-gain application of SP 800-171 requirements across system components based upon the constraints on where CUI can flow within the system and at the system boundary.	None	**Example:** Utilize network devices to limit the system to system access of CUI through switch policy, firewall rules, or segregation.

Adjust your Game Plan

- Agility
- Flexibility
- Adapt and overcome

"You improvise.
You adapt.
You overcome."

~ Clint Eastwood
Heartbreak
Ridge

Questions

Andrew Spragg

ags5008@arl.psu.edu

"I never learn anything talking. I only learn things when I ask questions." *Lou Holtz*