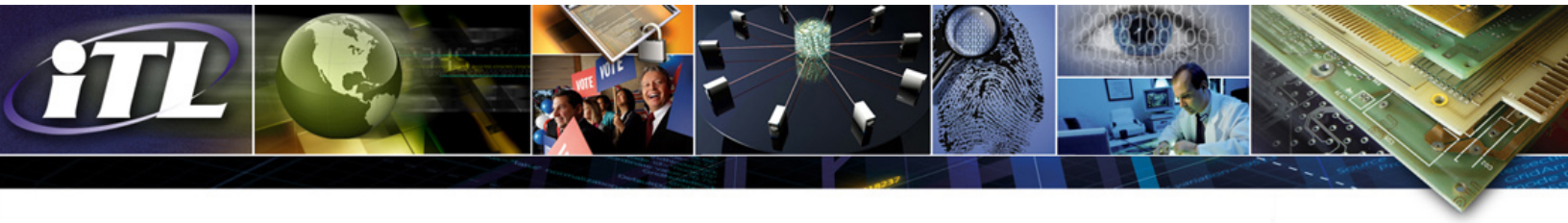


ITL BULLETIN FOR OCTOBER 2015

PROTECTION OF CONTROLLED UNCLASSIFIED INFORMATION

Ron Ross, Kelley Dempsey, Larry Feldman[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

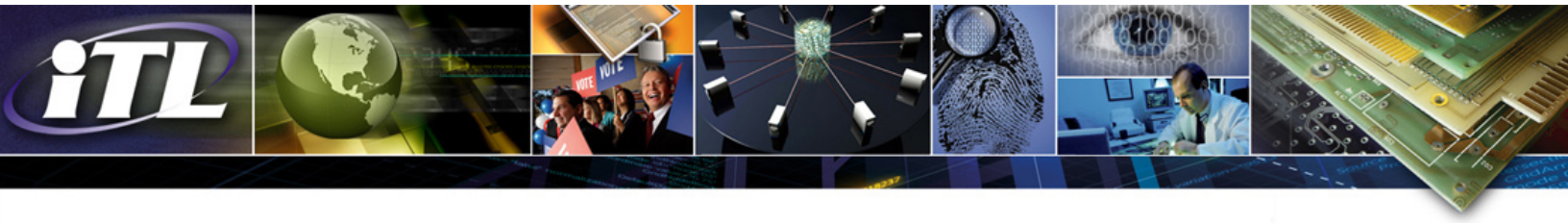
On November 4, 2010, the President signed Executive Order 13556, *Controlled Unclassified Information*.[2] It established a governmentwide Controlled Unclassified Information (CUI) Program to standardize the way the executive branch handles unclassified information that requires protection. The Executive Order also designated the National Archives and Records Administration (NARA) as the Executive Agent to implement that program. Only information that requires the safeguarding or dissemination of controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.

Introduction

While there is existing guidance for the protection of unclassified information within "federal information systems" (i.e., an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency), guidance was needed about how to protect CUI in *nonfederal* systems. Examples of nonfederal organizations include state, local, and tribal governments, colleges and universities, and contractors. The protection of nonfederal CUI is essential to federal agencies and can directly impact their ability to successfully carry out designated missions and business operations. NIST has released a new publication, Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, which provides requirements for protecting the confidentiality of CUI:

- When the CUI is resident in nonfederal information systems and organizations;
- When the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations *on behalf of* those agencies; or

[1] G2, Inc.
[2] http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf



- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

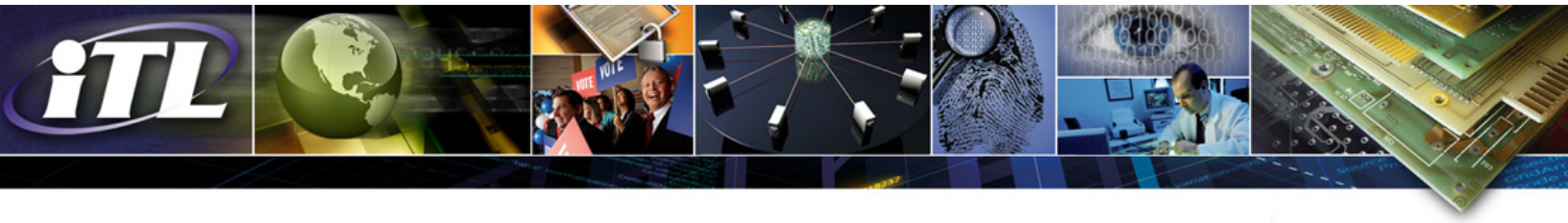
The Fundamentals

Federal information that is designated as CUI has the same intrinsic value and potential adverse impact if compromised whether such information resides in a federal or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies and the economic and national security interests of the nation. Additional assumptions also impacting the development of the CUI security requirements and the expectation of federal agencies in working with nonfederal entities include:

- Nonfederal organizations have information technology infrastructures in place, and are not necessarily developing or acquiring information systems specifically for the purpose of processing, storing, or transmitting CUI;
- Nonfederal organizations have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the CUI security requirements;
- Nonfederal organizations can implement a variety of potential security solutions either directly or through the use of managed services, to satisfy CUI security requirements; and
- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every CUI security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.

Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of: (i) a *basic security requirements* section; and (ii) a *derived security requirements* section. The basic security requirements are obtained from Federal Information Processing Standard (FIPS) 200, which provides the high-level and fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in SP 800-53. Starting with the FIPS 200 security requirements and the security controls in the moderate baseline (i.e., the minimum level of protection required for CUI in federal information systems and organizations), the requirements and controls are *tailored* to eliminate requirements, controls, or parts of controls that are:

- Uniquely federal (i.e., primarily the responsibility of the federal government);



- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.

Appendix E of SP 800-171 describes the criteria for tailoring the requirements and controls. The appendix provides seventeen tables that specify the particular tailoring actions taken. Drawing from the seventeen control families listed in SP 800-53, which are themselves closely aligned with the FIPS 200 security-related areas, SP 800-171 organizes the basic and derived security requirements into fourteen families.[3] While some controls may be tailored out from the CUI-specific requirements, these may still need to be included as part of an organization's security program.

The Requirements

The security requirements identified in the publication are intended to be applied to the nonfederal organization's general-purpose internal information systems that are processing, storing, or transmitting CUI. Some specialized systems, such as medical devices, Computer Numerical Control machines, or industrial control systems, may have restrictions or limitations on the application of certain CUI requirements and may be granted waivers or exemptions from the requirements by the federal agency providing oversight.

The security control references in Appendix D of SP 800-171 are included to promote a better understanding of the CUI security requirements. The appendix provides a direct mapping of the CUI security requirements to the security controls in SP 800-53 and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001. Once identified, those controls can also be used to reference the functions, categories, and subcategories used in the NIST Cybersecurity Framework.[4]

The control references are not intended to impose additional requirements on nonfederal organizations. Moreover, because the security controls referenced were developed for federal agencies, the supplemental guidance associated with those controls may not apply to nonfederal organizations.

Conclusion

SP 800-171 helps nonfederal entities, including contractors, to comply with the security requirements using the systems and practices they already have in place, rather than trying to use government-specific approaches. The publication provides a standardized and uniform set of requirements for all CUI security needs, tailored to nonfederal systems, allowing nonfederal organizations to be in compliance

[3] The contingency planning, system and services acquisition, and planning requirements are not included within the scope of SP 800-171 based upon the tailoring criteria in Appendix E.
[4] The NIST Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") is available from this website.

with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI.

NARA, in its capacity as the CUI Executive Agent, plans to sponsor a single Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the proposed federal CUI regulation and SP 800-171 to contractors. This will further promote standardization to benefit a substantial number of nonfederal organizations that are attempting to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from federal agencies for the same information gives rise to confusion and inefficiencies. Until the formal process of establishing such a single FAR clause takes place, the CUI requirements in SP 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements. If necessary, SP 800-171 will be updated to remain consistent with the proposed federal CUI regulation and the FAR clause.

Additional Resources

NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, June 2015.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST Framework for Improving Critical Infrastructure Cybersecurity website.

Controlled Unclassified Information (CUI) website (National Archives and Records Administration).

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov