

Family of Controls

Publication 4812 requires technical, operational, and managerial controls to ensure the protection of sensitive information. These include:

- Technical Controls
 - Access Control
 - Audit and Accountability,
 - Identification and Authentication, and
 - System and Communications Protection.
- Operational Controls
 - Awareness and Training,
 - Configuration Management,
 - Contingency Planning,
 - Incident Response,
 - Maintenance,
 - Media Protection,
 - Physical and Environmental Protection, and
 - Personnel Security.
- Management Controls
 - Security Assessment and Authorization,
 - Planning,
 - Risk Assessment,
 - System and Services Acquisition, and
 - System and Information Integrity.

The following control does not apply to contractors because the IRS is primarily responsible for Program Management controls.

- Program Management

Reference Links

Publication 4812

<http://www.irs.gov/uac/Publication-4812---Contractor-Security-Controls>

NIST 800-53 (Revision 3)

<http://csrc.nist.gov/publications/PubsSPs.html>

Internal Revenue Code Section 6103

<http://www.gpo.gov/fdsys/pkg/USCODE-2010-title26/html/USCODE-2010-title26-subtitleF-chap61-subchapB-sec6103.htm>

FISMA

<http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

Contact Us

Questions can be directed to:
Pub4812@irs.gov



IT Information Technology and
Cybersecurity

Infrastructure Security Reviews

Highlights of Publication 4812 *Contractor Security Controls*

What is IRS Publication 4812?

Publication 4812 is a new publication designed to identify security requirements for contractors and any subcontractors supporting the primary contract. This applies to contractors (and their subcontractors) who handle or manage Internal Revenue Service (IRS) information at contractor managed facilities on behalf of the IRS.

Sensitive But Unclassified (SBU) information includes all taxpayer returns and return information, as defined by Internal Revenue Code (IRC) Section 6103, all Personally Identifiable Information, where there is information that can be associated to a specific individual, and other sensitive information that should be organizationally sensitive, such as Information Technology system configurations, identification of vulnerabilities, etc.

The publication identifies requirements established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Revision 3) *Recommended Security Controls for Federal Information Systems and Organizations*, as amended.

Why was IRS Publication 4812 Created?

In 2001, the Office of Management and Budget (OMB) identified the security of contractor-provided services as a government-wide challenge in its information security report to Congress. When the Federal Information Security Management Act (FISMA) was enacted a year later, provisions and guidelines were included to ensure the effectiveness of information security controls that support

Federal operations and assets. FISMA requirements explicitly apply to all Federal contractors that possess or have direct access to agency information, or operate Federal information systems on behalf of an agency.

Who Needs Publication 4812?

The requirements in Publication 4812 and the security controls, based on NIST SP 800-53 (Revision 3), as amended, are applicable to IRS contractors and contractor personnel who possess or have access to Federal information or information systems, or are responsible for handling or processing Federal information or information systems pursuant to or in the course of performance of a contract, order, or agreement with the IRS. Typically, this publication is incorporated into IRS contracts, agreements or orders (directly or through flow down provisions), by reference. The target date for Publication 4812 compliance is the beginning of the next FISMA year, July 1, 2013.

Contractor Responsibilities

It is the responsibility of the IRS contractors to build effective security controls into their business environment, including IT security, personnel security, and physical security, in accordance with the terms of the contracts and as outlined in this publication.

Contractors are responsible for developing policies, procedures, and processes to define the required managerial, operational, and technical security controls that will be used to secure IRS information.

Contractors must maintain ongoing awareness of their information system and related security

control processes to ensure compliance with security controls and adequate security of information, and to support organizational risk management decisions.

State of Security Package

Contracts subject to Publication 4812 that are 12 months or more in duration, the contractor shall develop and submit a State of Security (SoS) package each period of performance of the contract (base and exercised option periods), or once every 12 months, whichever period is less. The SoS package is comprised of the following components:

- Contractor Statements of Security Assurance (CSSA),
- SoS Questionnaire, and
- System Security Plan.

Contractor Reviews

Contractor Security Reviews are on-site evaluations performed by the IRS to assess and validate the effectiveness of security controls established to protect IRS information and information systems. These assessments help to determine if and when additional controls or protections are necessary to protect returns and return information or personal privacy, or other SBU information, and organizational assets and operations.

The types of contractor reviews are:

- Pre-Award Reviews,
- Immediate (Probationary) Post-Award Reviews,
- Periodic Post-Award Reviews, and
- Closeout and Contractor Site Shutdowns.