Family of Controls

Publication 4812 (Rev. 7-2014) requires the following list of security control families and family identifiers to ensure the protection of sensitive information. These include:

- AC: Access Control,
- AT: Awareness and Training,
- AU: Audit and Accountability,
- CA: Security Assessment and Authorization,
- CM: Configuration Management,
- CP: Contingency Planning,
- IA: Identification and Authentication,
- IR: Incident Response,
- MA: Maintenance,
- MP: Media Protection,
- PE: Physical and Environmental Protection,
- PL: Planning,
- PS: Personnel Security,
- RA: Risk Assessment,
- SA: System and Services Acquisition,
- SC: System and Communications Protection, and
- SI: System and Information Integrity.

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

- PM: Program Management

Certain Privacy Controls are also relevant to this document. These include:

- AR: Accountability, Audit, and Risk Management
- DM: Data Minimization and Retention
- SE: Security

Reference Links

Publication 4812 (Rev. 7-2014)
http://www.irs.gov/pub/irs-procure/Publication-4812---Contractor--Security-Controls.pdf

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

Publication 4812-A (Rev. 9-2014) Catalog Number 62262W
Department of the Treasury **Internal Revenue Service** www.irs.gov

IRS Information Technology
CYBERSECURITY

Highlights of Publication 4812

Contractor Security Controls

What is IRS Publication 4812?

Publication 4812 (Rev. 7-2014) is a publication designed to identify security control requirements for contractors, and their subcontractors, who handle or manage Internal Revenue Service (IRS) Sensitive But Unclassified (SBU) and/or Personally Identifiable Information (PII) information at contractor managed facilities on behalf of the IRS.

SBU information includes; all taxpayer returns and return information, as defined by Internal Revenue Code (IRC) Section 6103; PII 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 uses security controls established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Revision 4) Security and Privacy Controls for Federal Information Systems and Organizations. The implementation of the selected controls is based on specific IRS requirements.

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 (Rev. 7-2014) and its security controls, which are based on NIST SP 800-53 (Revision 4), are applicable to contractors, and their subcontractors, and employees who handle or manage IRS, SBU and PII information at contractor managed facilities on behalf of the IRS.

Typically, this publication is incorporated into IRS contracts, agreements or orders (directly or through flow down provisions), by reference. All contracts should be following the guidance in the Policy and Procedures (P&P) document to ensure contract language is compliant with Publication 4812 (Rev. 7-2014).

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 families of 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

For contracts that are subject to Publication 4812 (Rev. 7-2014) (12 months or more in duration), the contractor shall develop and submit a State of Security (SoS) package. This will be done for 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:

- SoS Questionnaire,
- Contractor Statement of Security Assurance (CSSA),
- Contractor Statement of Physical Security (CSPSA), and
- System Security Plan.

Contractor Assessments

Contractor Security Assessments 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 assessments are:

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