



# Indiana Department of Revenue

## COMPLETE SECURITY ROADMAP

**Purpose:** Provide security guidance to vendors of tax e-filing products and services wishing to process Indiana taxpayer returns

### Background

The Indiana Department of Revenue (DOR) is committed to the maximum protection of taxpayer information. To realize this goal, DOR follows National Institute of Standards and Technology (NIST) security guidance and uses Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIG) checklists to technically implement it.

DOR requires tax e-filing vendors connecting to, transmitting data to, and receiving data from the department's network and systems to adhere to the same guidance. This document explains the roadmap those vendors must follow to comply with DOR's requirements.

### Definitions

- **Category (CAT) 1 Findings:** DISA STIG severity code indicating a finding's weakness enables primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges
- **CAT 2 Findings:** DISA STIG severity code indicating a finding's weakness can potentially lead to unauthorized system access or activity
- **CAT 3 Findings:** DISA STIG severity code indicating a finding's weakness can be addressed with recommendations to improve the security posture
- **Compensating Control:** Alternate control to address a security finding's weakness if the DISA-prescribed control cannot be implemented
- **DISA STIG:** Comprehensive technology-centric security checklists that align with NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-53:** Policy that defines how federal agencies will protect their information systems. IRS Publication 1075, which DOR must follow, is derived from this policy.
- **Plan of Action and Milestones (POAM):** For findings that are not resolved, POAMs are used to explain the pending solutions, whether DISA-prescribed or DOR-approved compensating control and the timelines to their implementation

### Roadmap Overview

DOR acknowledges that new tax e-filing vendors may need time to adapt to the department's security requirements. Consequently, DOR established a multi-year roadmap so they can become familiar with the expected processes and deliverables. DOR Security Team will also reach out to vendors to offer guidance and assistance. Vendors are strongly encouraged to contact DOR Security Team with any questions.

DOR reserves the right to conduct security audits of, and reject tax data from, any product or service that does not meet its security requirements.

## ROADMAP

### Year 1 Deadlines

- 1 Sep: Contact DOR Security Team at [IDOR Security Office@dor.in.gov](mailto:IDOR_Security_Office@dor.in.gov) to initiate roadmap and submit current product architecture—DOR Security Team will provide relevant STIG checklists
- 15 Oct: Submit results of assessment performed using STIG checklists
- 1 Dec: Submit a report of how CAT 1 findings are resolved, either in accordance with DISA prescribed solutions, DOR approved compensating controls, or POAMs

Recommendation: Vendors should start planning on how to resolve CAT 2 findings, and begin developing NIST-prescribed plans, policies, and procedures that are due in Year 3

### Year 2 Deadlines (Repeats Year 1 Deliverables)

- 1 Sep: Submit current product architecture—DOR Security Team will provide relevant STIG checklists
- 15 Oct: Submit results of assessment performed using STIG checklists
- 1 Dec: Submit a report of how CAT 1 findings are resolved, either in accordance with DISA prescribed solutions, DOR approved compensating controls, or POAMs

Recommendation: Vendors should have started working to resolve CAT 2 findings, and developing NIST-prescribed plans, policies, and procedures that are due in Year 3

### Year 3 Deadlines (Expands Upon Years 1 and 2 Deliverables)

- 1 Sep: Submit current product architecture—DOR Security Team will provide relevant STIG checklists
- 15 Oct: Submit new assessment using current STIG checklists to DOR Security Team
- 1 Dec: Submit the following
  - Report of how CAT 1 and 2 findings are resolved--either in accordance with DISA prescribed solutions, DOR approved compensating controls, or POAMs
  - Report of CAT 3 findings status
  - A letter signed by a legally responsible officer certifying each e-filing product meets the department's security requirements, and confirming that NIST-prescribed plans, policies and procedures are implemented (see below list)
  - Defined department update form

### Post Year 3

- In every following year, perform annual assessments using current STIG checklists
- In Year 4 and subsequent alternating years, provide a letter signed by a legally responsible officer certifying each e-filing product meets the department's security requirements, and confirming that NIST-prescribed plans, policies and procedures are implemented
- In Year 5 and subsequent alternate years, provide results of a new assessment using current STIG checklists that show CAT 1 and 2 findings resolved in accordance with DISA prescribed solutions, DOR approved compensating controls, or POAMs.

## NIST POLICIES, PROCEDURES, AND PLANS

The following comprises the 33 NIST plans, policies, and procedures that vendors must have in place for each of their e-filing products in Year 3. All documents are referenced in NIST SP 800-53, meaning they are NIST-prescribed security controls.

<b>Document Name</b>	<b>NIST 800-53 Reference</b>
Access Control (AC) Policy	AC-1 Access Control Policy and Procedure
Awareness and Training (AT) Policy	AT-1 Awareness and Training Policy and Procedure
Audit and Accountability (AU) Policy	AU-1 Audit and Accountability Policy and Procedure
Security Assessment and Authorization (CA) Policy	CA-1 Security Assessment and Authorization Policy and Procedure
Configuration Management (CM) Policy	CM-1 Configuration Management Policy and Procedure
CM Plan	CM-9 Configuration Management Plan
Contingency Planning (CP) Policy	CP-1 Contingency Planning Policy and Procedure
Contingency Plan	CP-2 Contingency Plan
Identification and Authentication (IA) Policy	IA-1 Identification and Authentication Policy and Procedure
Incident Response (IR) Policy	IR-1 Incident Response Policy and Procedure
Incident Response Plan	IR-8 Incident Response Plan
Maintenance (MA) Policy	MA-1 Maintenance Policy and Procedure
Media Protection (MP) Policy	MP-1 Media Protection Policy and Procedure
Physical and Environmental Protection (PE) Policy	PE-1 Physical and Environmental Protection Policy and Procedure
Planning (PL) Policy	PL-1 Planning Policy and Procedure Policy and Procedure
Personnel Security (PS) Policy	PS-1 Personnel Security
Risk Assessment (RA) Policy	RA-1 Risk Assessment Policy and Procedure
System and Services Acquisition (SA) Policy	SA-1 System and Services Acquisition Policy and Procedure
System and Communication Protection (SC) Policy	SC-1 System and Communications Protection Policy and Procedure
System and Information Integrity (SI) Policy	SI-1 System and Information Integrity Policy and Procedure
Program Management (PM) Policy	PM-1 Information Security Program Plan
System Security Plan	PL-2 System Security Plan
Security Objectives Categorization (FIPS 199)	1.1 Purpose and Applicability
Information System and Name Title	PL-2 System Security Plan
System Operational Status	PL-2 System Security Plan
System Function or Purpose	PL-2 System Security Plan
Information System Components and Boundaries	PL-2 System Security Plan PE-3 Physical Access SC-7 Boundary Protection
Type of Users and Roles	AC-2 Account Management AC-3 Access Enforcement PL-2 System Security Plan
Network Architecture	CA-3 System Interconnections
System Environment	PL-2 System Security Plan
External Systems Interconnects	AC-20 Use of External Information Systems PL-2 System Security Plan
User Guide	SA-5 Information System Documentation
Rules of Behavior	PL-4 Rules of Behavior PL-2 System Security Plan