Office of Privacy,
Governmental Liaison & Disclosure

# IRS Safeguards

## Federation of Tax Administrators

**Steve Matteson**
*steven.m.matteson@irs.gov*

**Megan Ripley**
*megan.j.ripley@irs.gov*

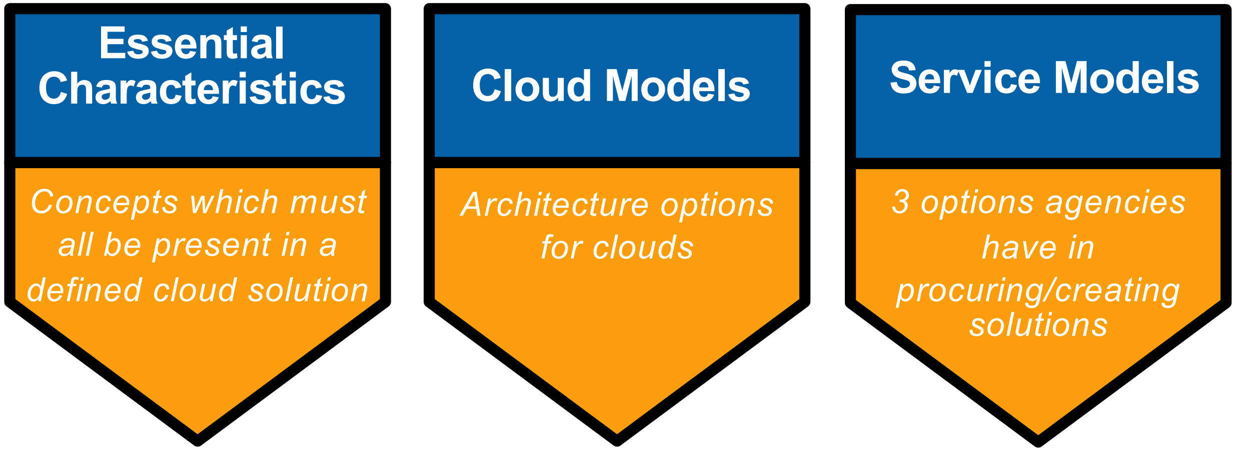
June 4, 2018
Nashville, TN

# Agenda

- Safeguards Requirements for Cloud Providers
- Using Nessus before, during, and after a Review
- Consolidated Data Center organizations and their participation in the Safeguards process
- Frequently Asked Questions

# What is a Cloud?

- NIST SP 800-175 defines essential characteristics, cloud models, and service model types for cloud computing.



## Essential Characteristics

*Concepts which must all be present in a defined cloud solution*

## Cloud Models

*Architecture options for clouds*

## Service Models

*3 options agencies have in procuring/creating solutions*

- On Demand Self Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

# Scoping Service Models

**Software as a Service (SaaS)**

- Using the provider's applications running on the provider's cloud infrastructure.
  - Provider is responsible for the highest amount of security and data protection under this model
  - Customer will negotiate into the service contract with the provider
- ***Safeguards Scoping Discussion***:
  - Least amount of controls for agency to implement and test: primarily, Access Control, Auditing, System Communication (Encryption)
  - Suggested SCSEM: Cloud SCSEM and applicable worksheets (e.g., Office 365)

**Platform as a Service (PaaS)**

- Deploying customer-created or acquired applications created using programming languages and tools supported by the provider.
  - Security is a shared responsibility with the provider responsible for the underlying platform infrastructure
  - Customer is responsible for securing the applications developed and hosted on the platform
- ***Safeguards Scoping Discussion:***
  - Moderate amount of controls for agency to implement and test: App development change management, database architecture, in addition to AC, AU, SC
  - Suggested SCSEM: Cloud SCSEM, Application SCSEM, Database SCSEM

# Scoping Service Models, cont’d.

Infrastructure as a Service (IaaS)

- Provision processing, storage, networks, and other fundamental computing resources.
  - Customer is responsible for the highest amount of security and data protection under this model.
- ***Safeguards Scoping Discussion***:
  - Agency has the most controls to implement and test in this model. Agencies may be responsible for implementing configurations of: OS, DBMS, and web server technical configurations
  - Suggested SCSEM: OS, DBMS, Application, Web Server, Boundary Protection (i.e., Firewall/VPN)

*Note: Clouds differ from Consolidated Data Centers as we typically do not see agencies or state entities (e.g., Departments of IT) managing the following devices within a Cloud: Hypervisors, Storage, Networking, or Remote access*

*Cloud provider security controls for networking, workstations, etc. are typically inherited from the cloud provider’s SSP and not assessed as part of a Safeguards review*

# Cloud Providers: Cloud Requirements

To utilize a cloud computing model to receive, transmit, store, or process FTI, the agency must be in compliance with all Publication 1075 requirements. The following mandatory requirements are in effect for introducing FTI to a cloud environment:

- Physical Description
- **FedRAMP Authorization**
- Notification Requirement
- Data Isolation
- Persistence of Data in Relieved Assets
- **Onshore Services**
- Service Level Agreements (SLA)
- Risk Assessment
- Multi-Factor Authentication
- Security Control Implementation
- **Data Encryption in Transit**
- **Data Encryption at Rest**

**FedRAMP Authorization**
Agencies maintaining FTI within cloud environments must engage services from FedRAMP certified vendors to complete the authorization framework resulting in an Authority to Operate.

**Onshore Services**
Agencies must leverage vendors and services where all Federal Tax Information resides physically in systems located within the United States.

**Encryption Requirements**
FTI must be encrypted in transit and at rest within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module.

# Safeguards in the Cloud

***If the agency is using a contractor or subcontractor in the cloud, the agency must notify Safeguards.***

## Third Party Solutions that *are* considered clouds

### Traditional Cloud Services

Instances where an agency has contracted with well-known public cloud vendors for supporting/implementing FTI systems.

Examples include:

- Google docs/email/apps
- Amazon Web Services
- MS365, MS Azure

### Data Storage Solutions

Instances where an agency uses third-party provided data storage and movement systems which meet cloud definition (multi-tenant, multiple facilities, etc.).

Examples include:

- Box.com
- Dropbox

## Third Party Solutions that *may not* be considered clouds

### Contracted Third Party Services

Instances where an agency has contracted a specific business process which a third party implements using their own technology.

Examples include (but not limited to):

- Collections Agencies
- Call Centers
- Field offices
- Print facilities

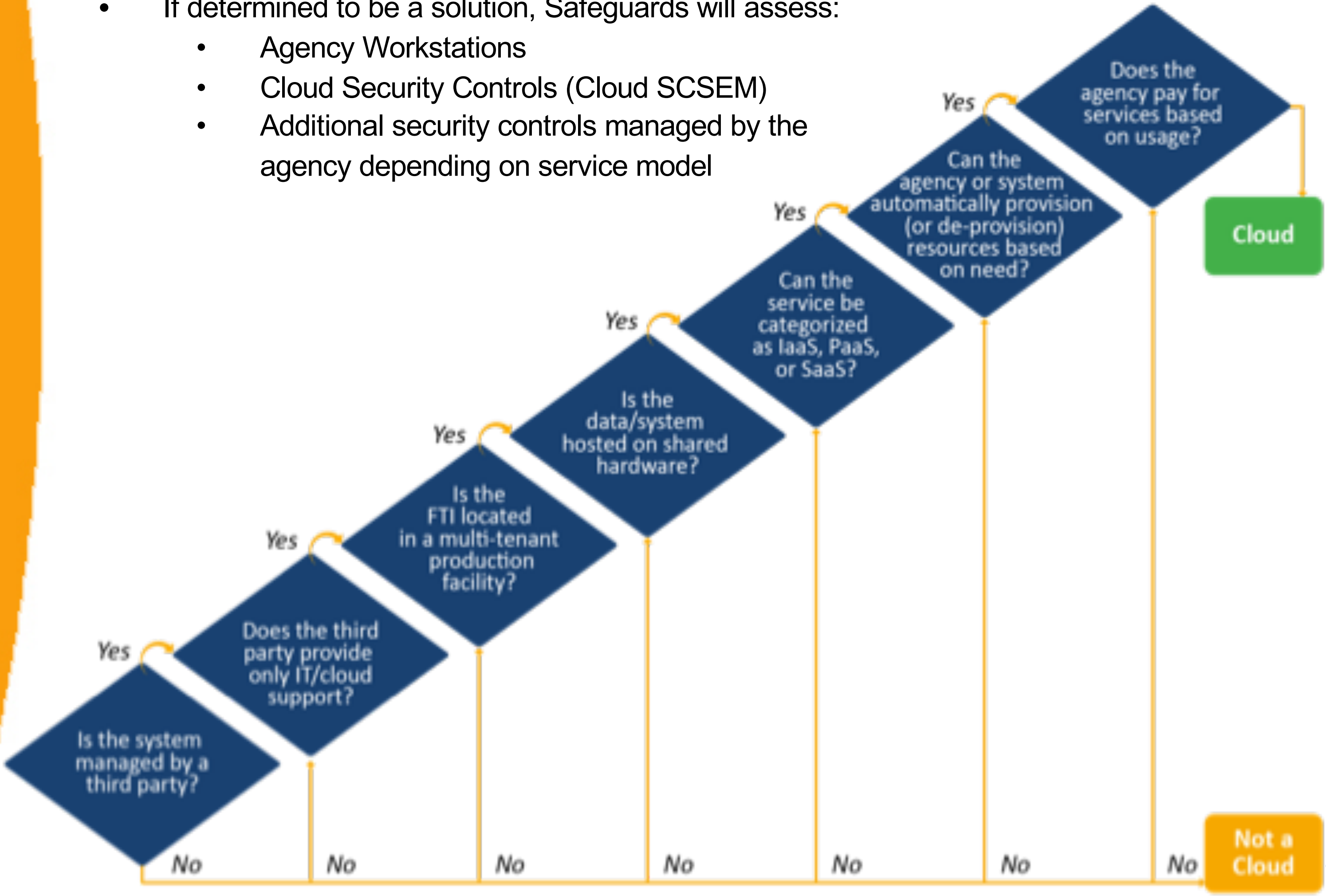
### Hosted Solutions

Instances where an agency maintains the ownership and configuration of technologies that are located in a third party-managed facility.

- Agency only relies on the third party solely for network connectivity, rack space, power, and cooling.
- Agency maintains root-level controls of the technologies used to process FTI.

# IT Scoping: Cloud vs Virtual System

- Safeguards uses criteria to determine whether a technical solution is in a Cloud environment or is within a Virtual Environment
- Agencies must provide a Cloud Computing Notification **45 days prior to implementation**
- If determined to be a solution, Safeguards will assess:
  - Agency Workstations
  - Cloud Security Controls (Cloud SCSEM)
  - Additional security controls managed by the agency depending on service model



Is the system managed by a third party?

Does the third party provide only IT/cloud support?

Is the FTI located in a multi-tenant production facility?

Is the data/system hosted on shared hardware?

Can the service be categorized as IaaS, PaaS, or SaaS?

Can the agency or system automatically provision (or de-provision) resources based on need?

Does the agency pay for services based on usage?

Cloud

Not a Cloud

# Preparing for the On-Site Review of a Cloud Solution

- Safeguards has released an updated Cloud Computing SCSEM which is available on the Safeguards website (www.irs.gov/uac/Safeguards-Program) in-line with the requirements listed in IRS Publication 1075 and other best practices
  - Safeguards has worked with Microsoft to create an Office 365 specific set of test cases and is working to finalize Azure test cases
  - Safeguards is in contact with Google and Amazon to create additional solution-specific test cases
  - More specific vendors and/or technologies may be added in the future
- Safeguards will evaluate SLAs, contracts, etc. established with the Service provider, in addition to evaluating security controls implemented by the agency. The nature of the agency-provided controls will depend on the Service Model in use.

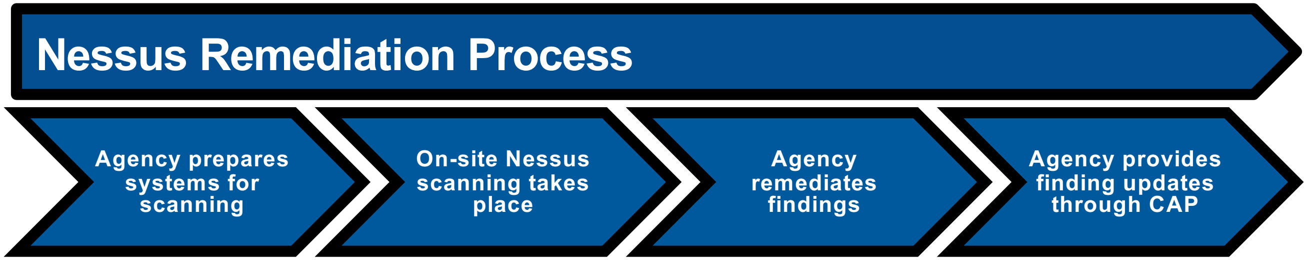
- Safeguards has the following positions related to cloud computing:
  - If FTI is in a non-FedRAMP cloud, **Safeguards will consider the cloud a critical finding.**
  - If FTI is found to be offshore in the cloud environment**, Safeguards will consider the cloud a critical finding**

# Nessus Scanning

**Overview**

- The Office of Safeguards uses Tenable’s Nessus to perform compliance testing.
- Nessus scan results will be left with the agency or third party during the on-site review.
- Agencies, third-parties, and data center organizations must prepare systems for assessment prior to the on-site review.
- Agencies can submit Nessus files as CAP evidence and need to provide the .Nessus, .csv, and .html output with the submission.
- Safeguards audits systems using the CIS Level 1 benchmark with modifications to meet IRS Publication 1075 and Internal Revenue Manual requirements.
- Failure to assess will result in a critical finding that could lead to a recommendation to terminate the contract or result in a potential (p)(7).

# Nessus Scanning



## Nessus Remediation Process

**Agency prepares systems for scanning**

- Identify System IP/Hostname
- Create Credentials
- Open Required Network Ports/Protocols

**On-site Nessus scanning takes place**

- Provide scan technician and work location
- Make other personnel (system admins, DBAs, networking engineers, desktop support) available for troubleshooting

**Agency remediates findings**

- Review recommendations and implement changes per configuration management program
- Re-scan systems using agency Nessus license, if applicable, using Safeguards audit profiles

**Agency provides finding updates through CAP**

- Describe changes in CAP document
- Provide evidence in the form of screenshots, updated configuration files, or complete Nessus results

## Available Resources to Support Nessus Scans

- IRS Office of Safeguards Website includes documentation on how to prepare individual systems for Scans https://www.irs.gov/pub/irs-utl/Preparing%20for%20Nessus%20Compliance%20Scanning.pdf
- Safeguards scan templates and audit files can be downloaded from the Safeguards website
- Agencies may email the Safeguards Mailbox (safeguardreports@irs.gov) to ask a question and receive either a written response or a conference call / working session
- Dial into upcoming Office Hours calls in June to discuss the configuration and use of Nessus

# Nessus Scanning: Potential Pitfalls

- Registry keys and other configuration elements need to be explicitly set and configured to meet Safeguards requirements. Using defaults or unconfigured items will lead to Nessus determining a NULL result which cannot be accepted.
- Agencies should prepare their systems and personnel to avoid any scanning issues during the on-site review. This checklist should serve as a tool to help prepare agencies for on-site automated Nessus testing:

1. **Identify Personnel to support the review:**
   - Scan technicians, network technicians, system administrators, database administrators, and desktop services personnel are required to support Nessus activities
2. **Create scope inventory document**
   - OS version, hostname, IP address
3. **Define network location for scanning, whitelist scan engine**
   - Connectivity to target systems
4. **Create credentials**
   - Admin (or root) username/password at domain and/or local level
   - Include credential in security groups (Unix)
5. **Prepare systems - examples include:**
   - Disable UAC, enable remote registry and WMIC, open ports, test credentials
   - Disable lockdown mode
   - Enable SSH

- When performing test scans prior to an onsite visit, ensure scans are successful by validating the existence of “Compliance Details” for each host. Compliance details must be gathered in order for Safeguards to complete the assessment.

# State Consolidated Data Centers

## Why are Consolidated Data Centers relevant to the Safeguards conversation?

Many states have introduced data center consolidation to support Departments of Revenue in addition to other agency types which receive, process, store, or maintain FTI.

Participation from the Data Center management organization (i.e., Department of IT) needs to happen at the early stages of planning. A representative from the data center must be present on the PSE call and be listed on the PSE form to support preparation activities.

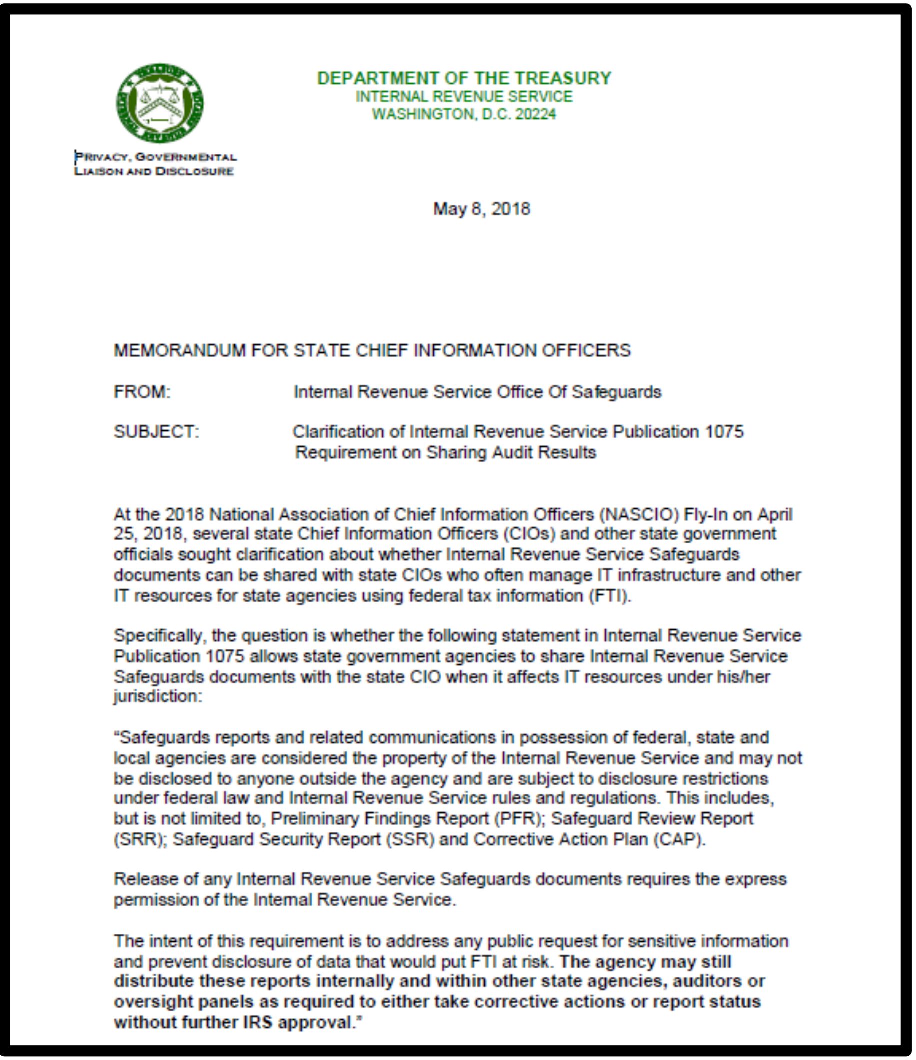
Agencies must coordinate with their Departments of IT to support onsite review logistics and CAP responses. Onsite logistics include scheduling, location, and preparation for Nessus scans for any devices in scope.

## Other Scope Factors introduced by Consolidated Data Centers

- **Contractors**: Departments of IT leverage contracting organizations to perform network services, DBA activities, etc. Contractors must be disclosed to Safeguards.
- **Back-up sites**: FTI may be located offsite requiring a physical review of the location and potential IT review of backup systems.
- **Physical protections**: Consolidated Data Centers must implement physical controls to meet the needs of all of its constituent agencies.

# State Consolidated Data Centers

As stated in the language of Publication 1075, Internal Revenue Service does allow for the sharing of Safeguards documents with state CIOs and others within state government as necessary; this does not require additional or further approval from Internal Revenue Service.



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

May 8, 2018

MEMORANDUM FOR STATE CHIEF INFORMATION OFFICERS

FROM: Internal Revenue Service Office Of Safeguards

SUBJECT: Clarification of Internal Revenue Service Publication 1075 Requirement on Sharing Audit Results

At the 2018 National Association of Chief Information Officers (NASCIO) Fly-In on April 25, 2018, several state Chief Information Officers (CIOs) and other state government officials sought clarification about whether Internal Revenue Service Safeguards documents can be shared with state CIOs who often manage IT infrastructure and other IT resources for state agencies using federal tax information (FTI).

Specifically, the question is whether the following statement in Internal Revenue Service Publication 1075 allows state government agencies to share Internal Revenue Service Safeguards documents with the state CIO when it affects IT resources under his/her jurisdiction:

"Safeguards reports and related communications in possession of federal, state and local agencies are considered the property of the Internal Revenue Service and may not be disclosed to anyone outside the agency and are subject to disclosure restrictions under federal law and Internal Revenue Service rules and regulations. This includes, but is not limited to, Preliminary Findings Report (PFR); Safeguard Review Report (SRR); Safeguard Security Report (SSR) and Corrective Action Plan (CAP).

Release of any Internal Revenue Service Safeguards documents requires the express permission of the Internal Revenue Service.

The intent of this requirement is to address any public request for sensitive information and prevent disclosure of data that would put FTI at risk. **The agency may still distribute these reports internally and within other state agencies, auditors or oversight panels as required to either take corrective actions or report status without further IRS approval.**"

# FAQ

Q

**Question 1:** Can we provide after hour / weekend Nessus scan results as part of our assessment?

A

Scans must be performed during the onsite review hours and must be observed by a member of the IRS Safeguards team.

Q

**Question 2:** Can we use an agency-provided Nessus license?

A

Yes; in addition to the observation requirement, the agency must use Safeguards audit profiles and must provide the .Nessus, .csv, and .html output from each scan task.

Q

**Question 3:** If our FTI is in a FedRAMP certified cloud, do the systems still need to be reviewed?

A

Yes, at the very least the Cloud SCSEM will need to be reviewed during the onsite assessment. Based on the services provided, additional SCSEMs would be brought into scope.

Q

**Question 4:** How can I limit the review of my third-party systems?

A

Agencies may allow external information systems to connect to their environments through well-configured VDI as described in Publication 1075 section 9.4.13. Third-party systems strictly using VDI to gain access to the FTI systems are not included in the scope of a review.

# FAQ

Q

**Question 5:** Can I send our PFR and SRR to our consolidated data center POCs for remediation?

A

Yes, the Safeguards Office will only provide reports directly to the agency. If only a portion of the CAP should be shared with a vendor or data center, an unlocked version can be requested from the Safeguards mailbox.

Q

**Question 6:** Why were my IT department's workstation images included in the scope of the review? They do not access FTI.

A

Administrator workstations are included in scope because they have access to systems where FTI is received, processed, stored, or maintained and could adjust the security features of those systems.

# Department of the Treasury
# Internal Revenue Service

[www.irs.gov](www.irs.gov)

# IRS Office of Safeguards

[www.irs.gov/uac/Safeguards-Program](www.irs.gov/uac/Safeguards-Program)