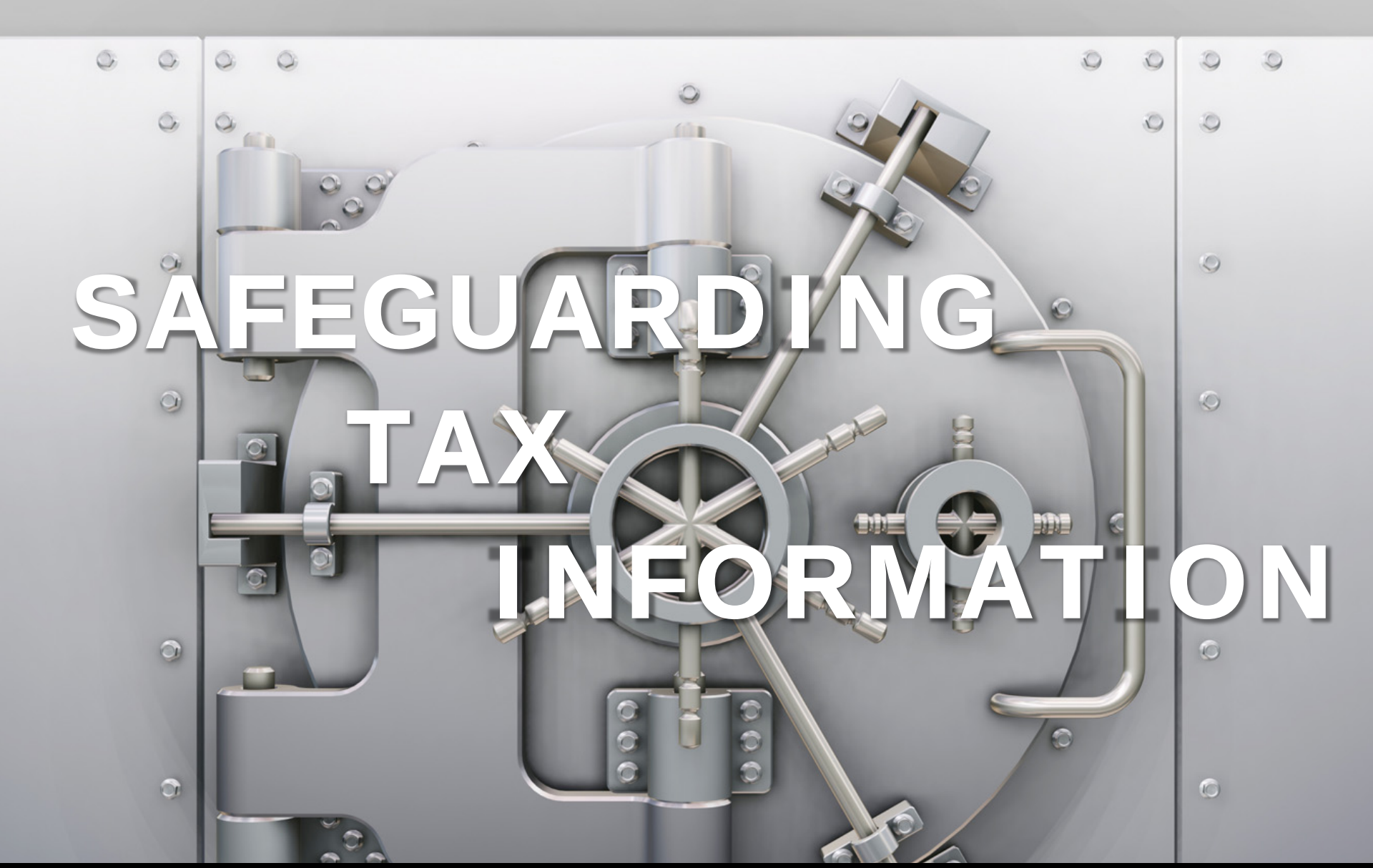


Lesson contains audio
Headphones recommended

Returns

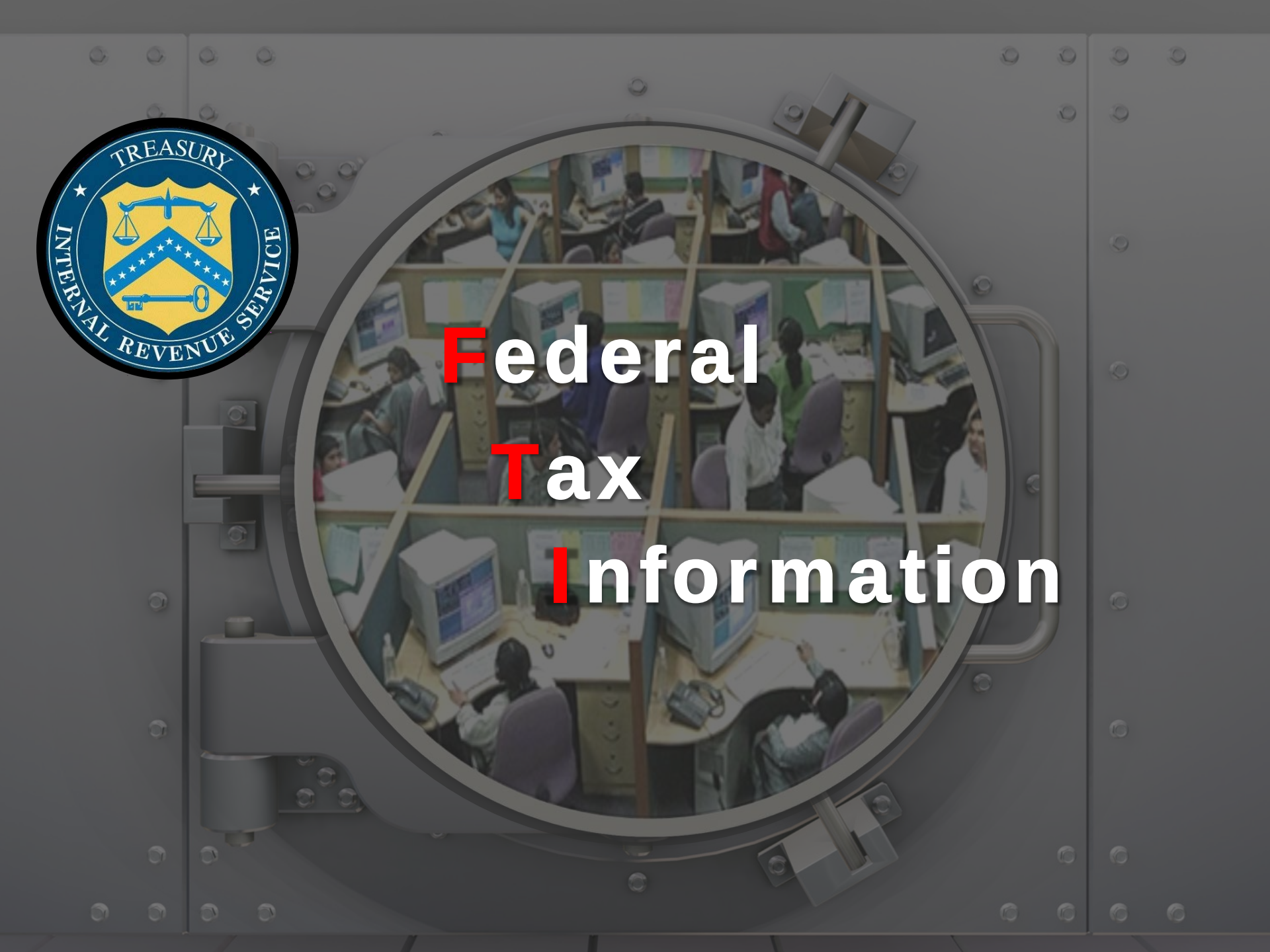
Payments

Correspondence

Conversations

Audit Reports

Notes


Federal
Tax
Information

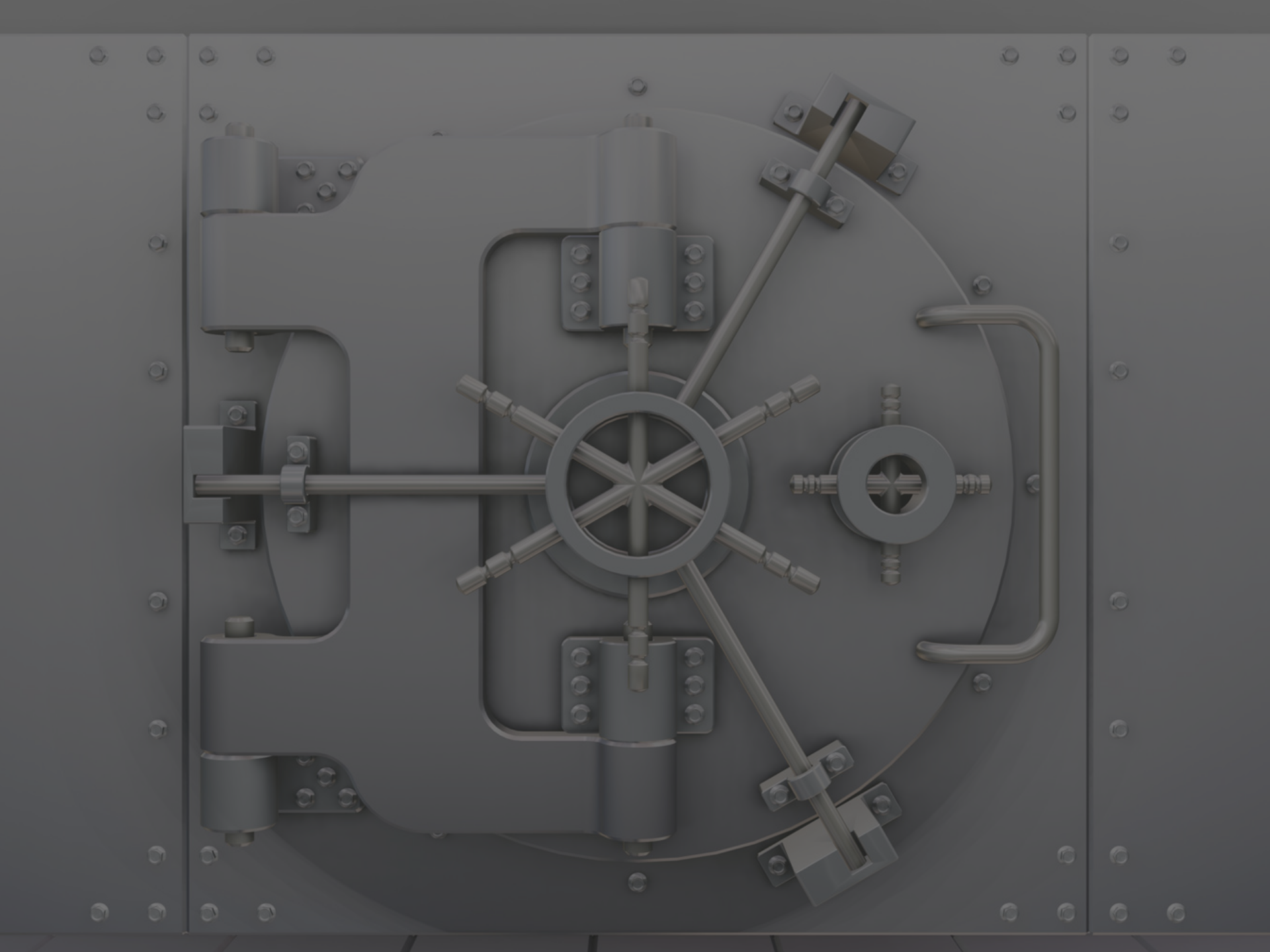

TREASURY
INTE
NAL REVENUE SE
VICE
TAX
VIRGINIA DEPARTMENT OF TAXATION

What co

Where

How t on

When t disclosures



Locate non-filers

Identify potential audit candidates

UNAX

Unauthorized Access and Inspection of Taxpayer Information

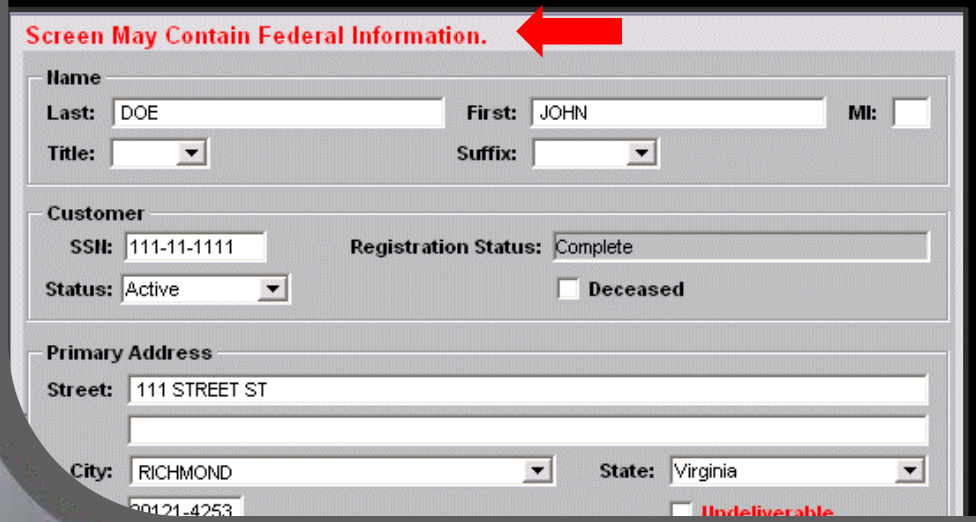
Revenue Agent Reports
Federal Transcripts

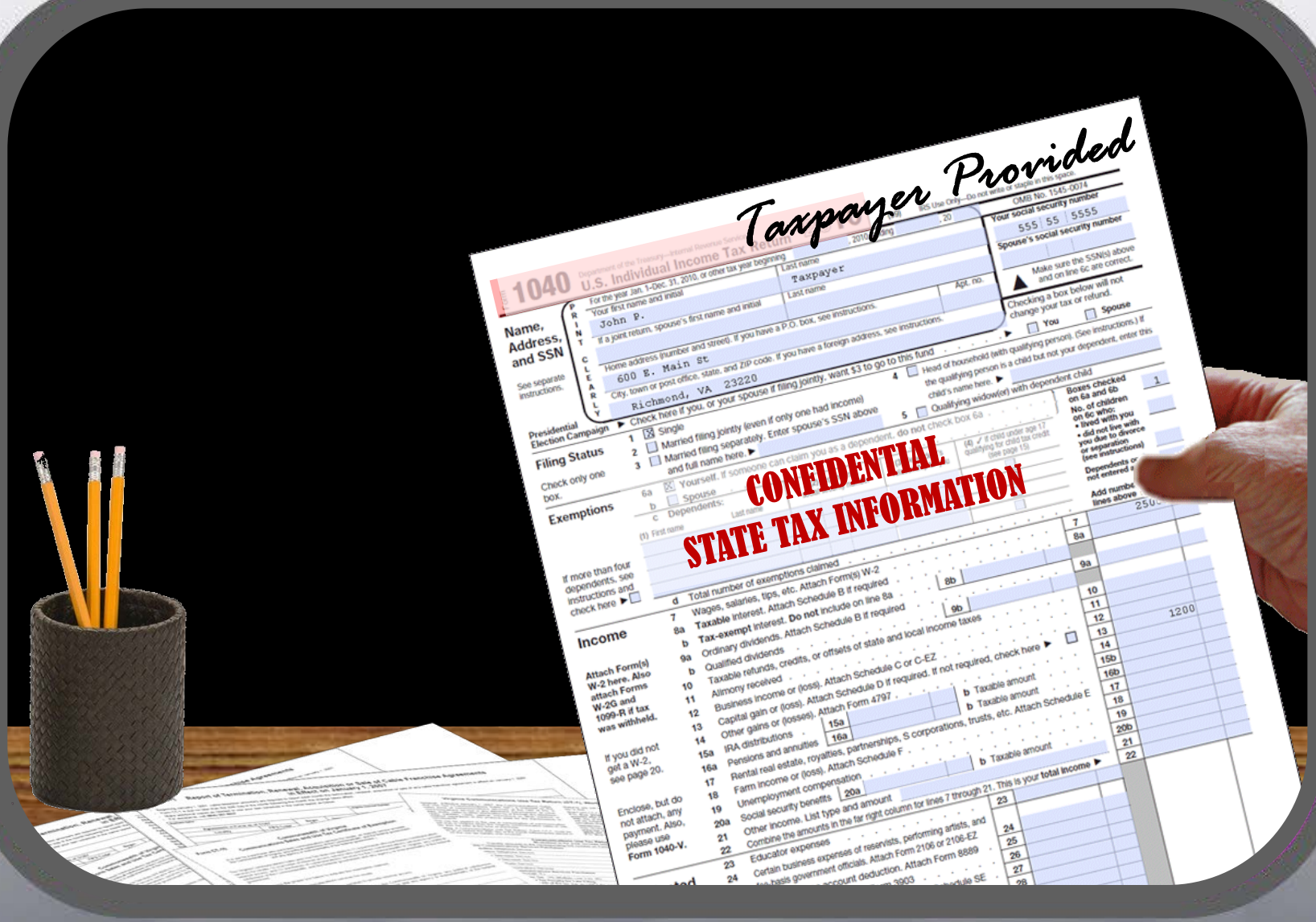
ADVANTAGE Revenue

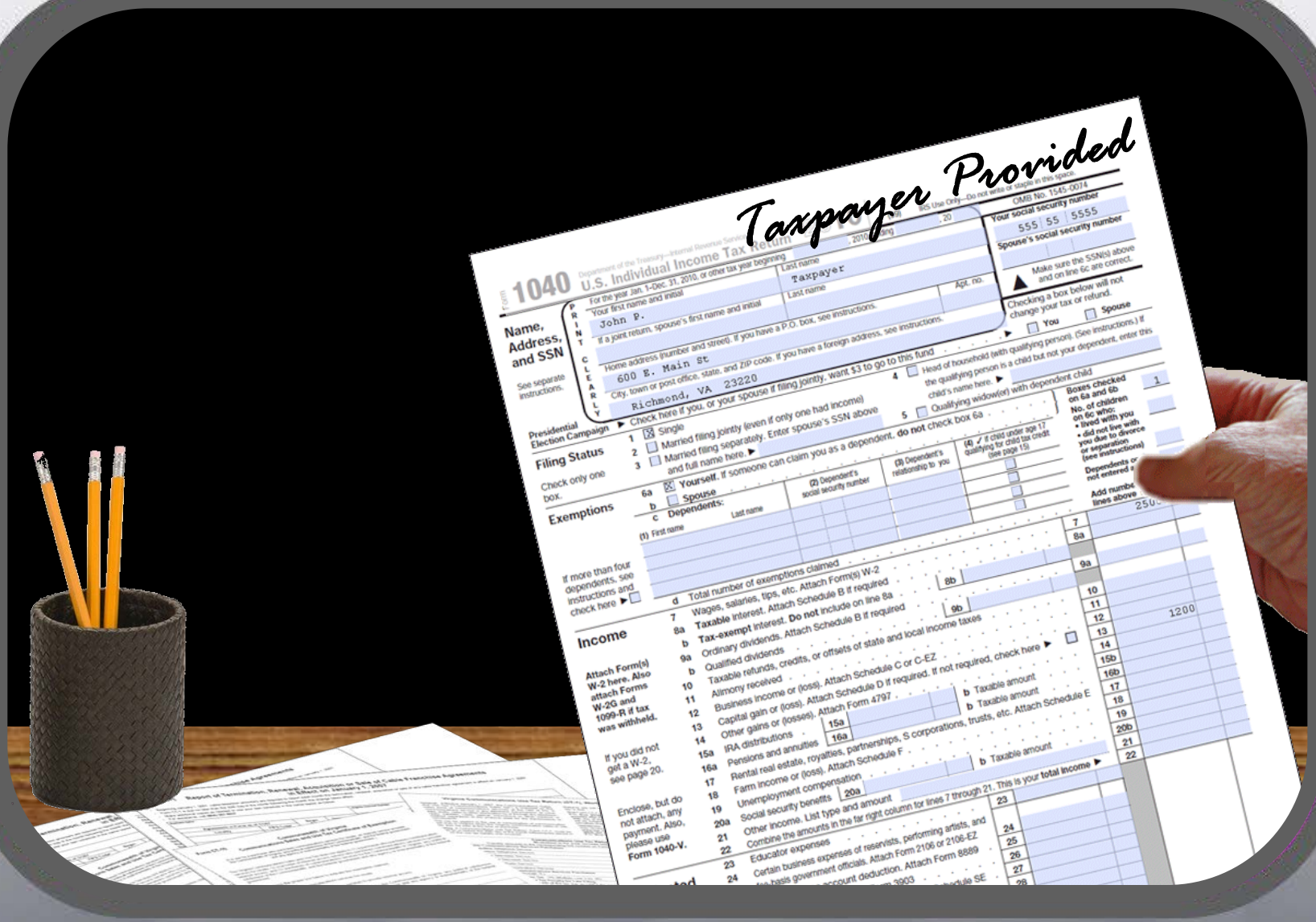
Siebel

CACSG

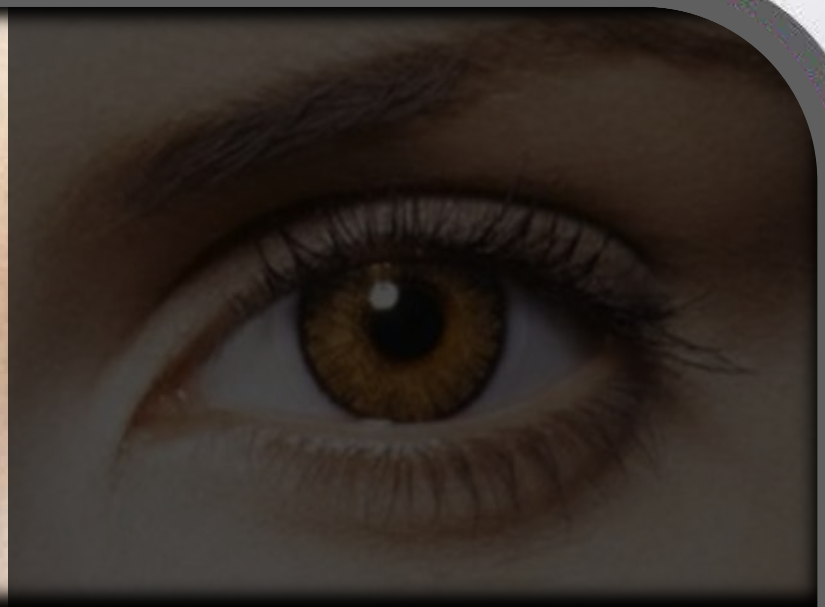
Compliance Repository




Taxpayer Provided
CONFIDENTIAL
STATE TAX INFORMATION
1040
U.S. Individual Income Tax Return
Name, Address, and SSN
Filing Status
Exemptions
Income
John P.
Taxpayer
600 E. Main St
Richmond, VA 23220
555 55 5555


Taxpayer Provided
Form 1040
U.S. Individual Income Tax Return
Name, Address, and SSN
John P.
Taxpayer
600 E. Main St
Richmond, VA 23220
Your social security number
555 55 5555
Filing Status
Exemptions
Income
Total number of exemptions claimed
Wages, salaries, tips, etc. Attach Form(s) W-2
Ordinary dividends. Attach Schedule B if required
Taxable refunds, credits, or offsets of state and local income taxes
Alimony received
Business income or (loss). Attach Schedule C or C-EZ
Capital gain or (loss). Attach Form 4797
Other gains or (losses). Attach Form 4797
IRA distributions
Pensions and annuities
Rental real estate, royalties, partnerships, S corporations, trusts, etc. Attach Schedule E
Farm income or (loss). Attach Schedule F
Unemployment compensation
Social security benefits
Other income. List type and amount
Combine the amounts in the far right column for lines 7 through 21. This is your total income
1200

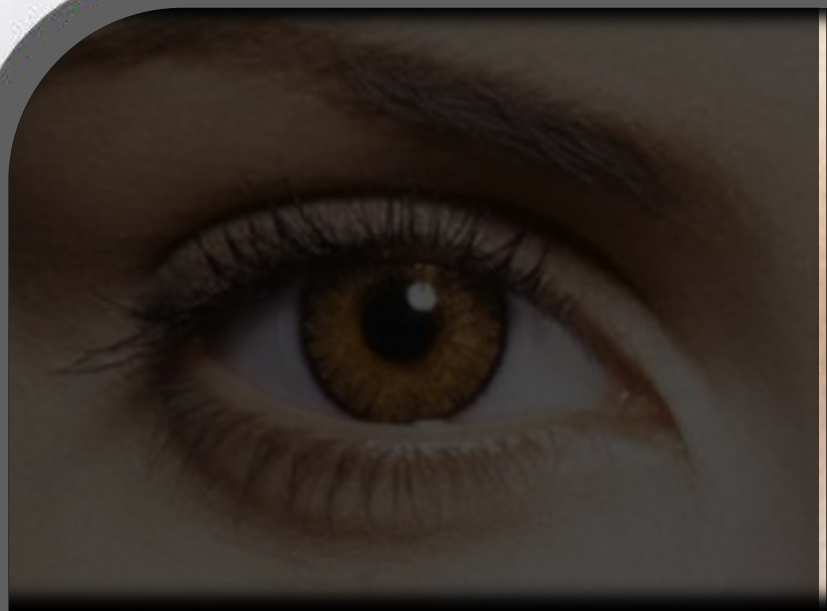
DISCLOSURE

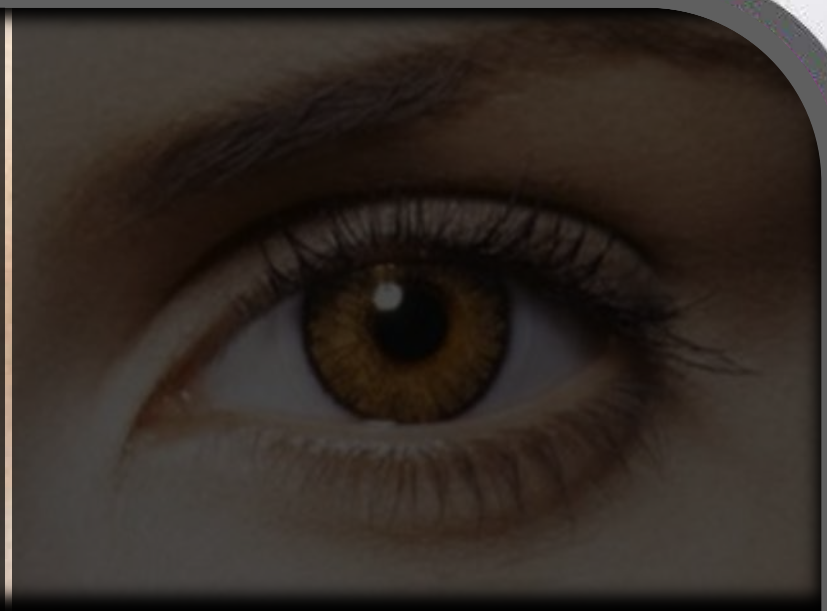


DISCLOSURE

Authorized Disclosure

- TAX Employees
- Taxpayers
- Third Parties with POA





Authorized Disclosure

- TAX Employees
- Taxpayers
- Third Parties with POA

Unauthorized Disclosure

- Inadvertent / Unintentional
- Advertent / Intentional

UNAUTHORIZED DISCLOSURE

Browsing = Unauthorized Disclosure

brows•ing (*brouz-ing*) The access or examination of confidential tax records without an assignment or business reason for doing so. *See also UNAX.*

Viewing your tax records

Viewing taxpayer information without a work related reason

- **Friends**
- **Neighbors**
- **Acquaintances**
- **Celebrities / VIPs**

Browsing = Unauthorized Disclosure

brows•ing (*brouz-ing*) The access or examination of confidential tax records without an assignment or business reason for doing so. *See also UNAX.*

Viewing your tax records

Viewing taxpayer information without a work related reason

- **Friends**
- **Neighbors**
- **Acquaintances**
- **Celebrities / VIPs**

Tax Code of Virginia

Section 58.1 Secrecy of Information; Penalties

Except in accordance with proper judicial order or as otherwise provided by law, the Tax Commissioner or agent, clerk, commissioner of the revenue, treasurer, or any other state or local tax or revenue officer or employee, or any former officer or employee of any of the aforementioned offices shall not divulge any information acquired by him in the performance of his duties with respect to the transactions, property, including personal property, income or business of any person, firm or corporation.

Such prohibition specifically includes any copy of Federal returns or Federal return information required by Virginia law to be attached to or included in the Virginia return.

Any person violating the provisions of this section shall be guilty of a Class 2 misdemeanor.

Notes

Applies to:

- TAX Commissioner, Agent, or Clerk
- Commissioner of Revenue
- Treasurer
- State or Local Tax Employee
- Former Employees

Protects Federal and State Return Data:

- Transactions
- Property
- Business, Corporate, Individual Income

Penalty

- Class 2 Misdemeanor

Internal Revenue Code

Section 6103: Confidentiality and Disclosure of Returns and Return Information

General Rule - Returns and return information shall be confidential, and except as authorized by this title:

1. no officer or employee of the United States

2. no officer or employee of any State, any local child support enforcement agency, or any local agency administering a program listed in subsection (1)(7)(D) who has or had access to returns or return information under this section, and

3. no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), paragraph (2) or (4)(B) of subsection (m) or subsection (n)

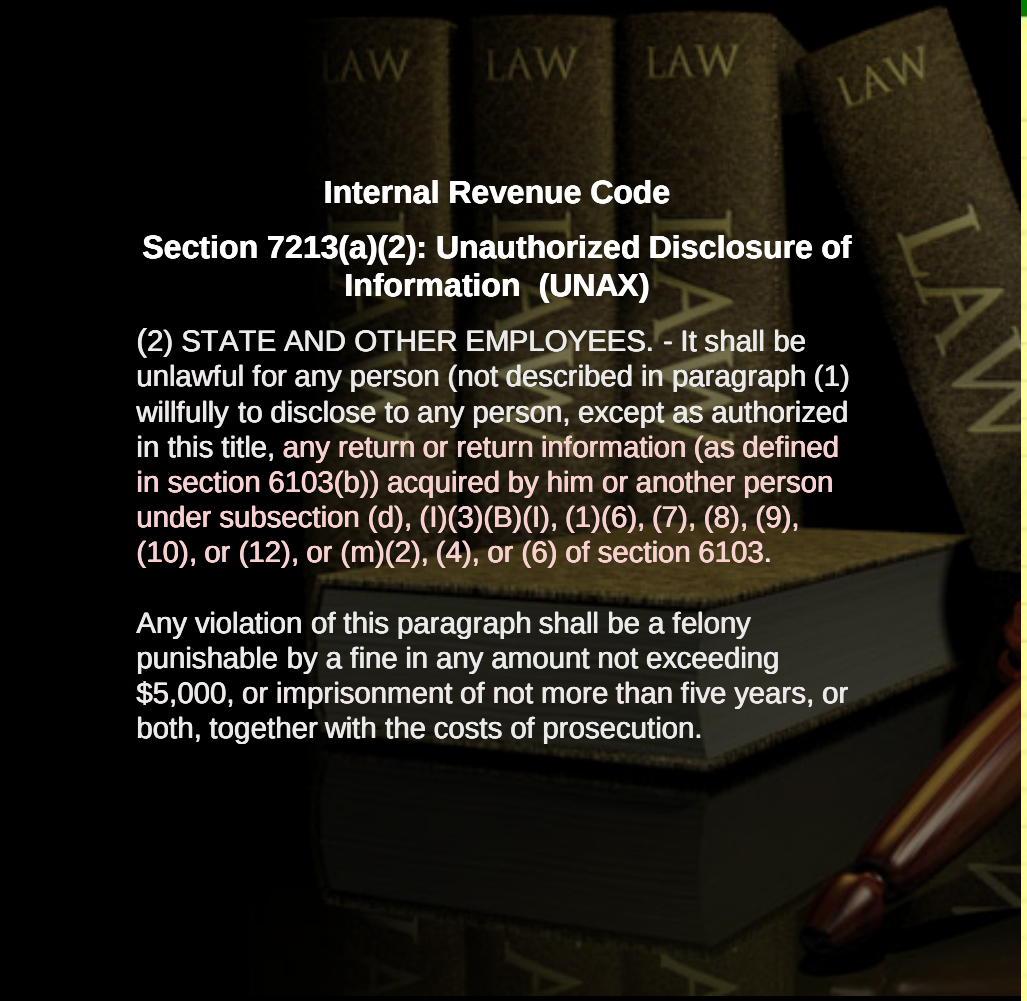
shall disclose any return or return information obtained by him in any manner in connection with his service. For purposes of this subsection, the term "officer or employee" includes any former officer or employee..

Notes

Defines return information as confidential

Extends disclosure to:

- U.S. Officers/Employees
- State and Local Officers/Employees
- ANY person with access to returns
- All former Officers/Employees



Internal Revenue Code

Section 7213(a)(2): Unauthorized Disclosure of Information (UNAX)

(2) STATE AND OTHER EMPLOYEES. - It shall be unlawful for any person (not described in paragraph (1) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (l)(3)(B)(l), (1)(6), (7), (8), (9), (10), or (12), or (m)(2), (4), or (6) of section 6103.

Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than five years, or both, together with the costs of prosecution.

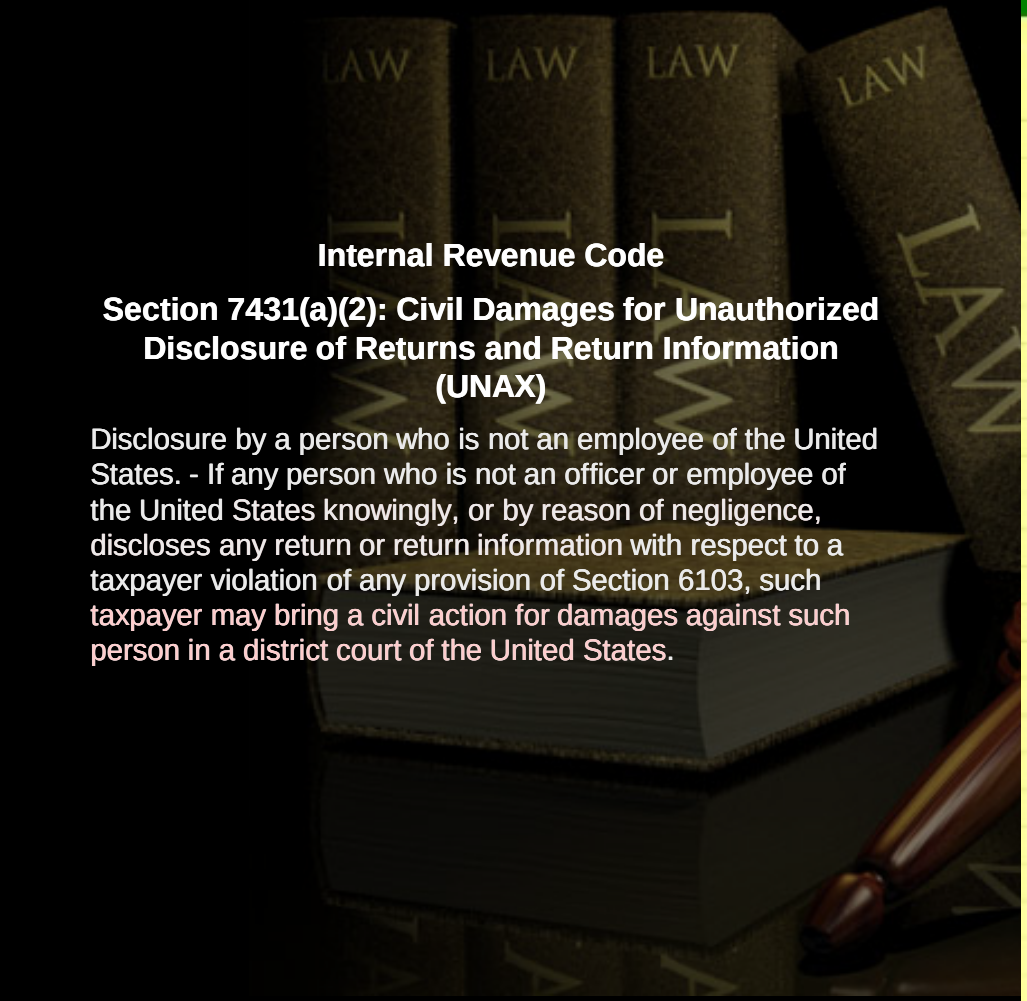
Notes

Makes disclosure unlawful to ANY person unless authorized by law

Defines return
- Tax information
- Estimated tax declarations
- Refund claims

Defines return information
- Liabilities, interest, fines, forfeitures
- Taxpayer's name, addresses
- Identification numbers
- Dependent names
- Return disposition

Felony
- Fines up to $5000
- Imprisonment up to 5 years
- Cost of prosecution



Internal Revenue Code

Section 7431(a)(2): Civil Damages for Unauthorized Disclosure of Returns and Return Information (UNAX)

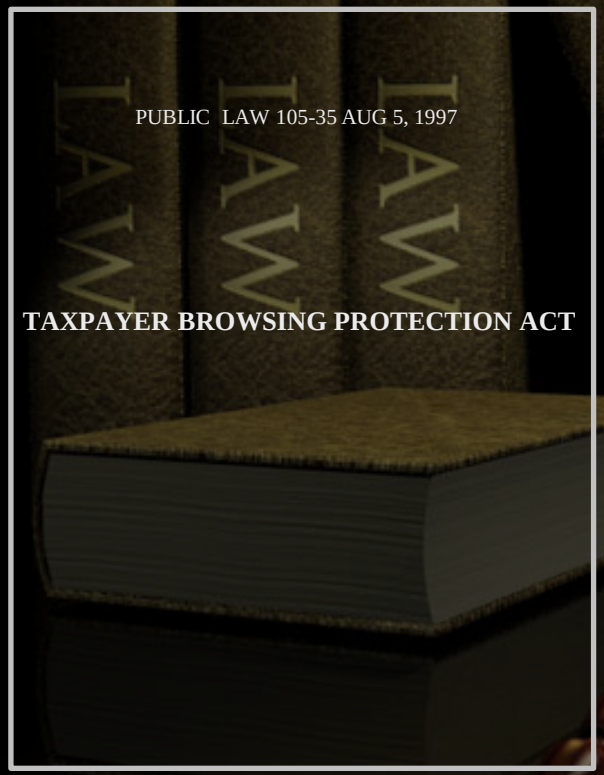
Disclosure by a person who is not an employee of the United States. - If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, discloses any return or return information with respect to a taxpayer violation of any provision of Section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

Notes

Broadens disclosure definition to include negligence

Allows taxpayer to seek civil damages

Taxpayer Browsing Protection Act (1997)



Notes

Civil damages for unauthorized inspection or disclosure.

Taxpayer may receive damages of $1000 or actual damage amount

Jail terms up to six months

Notes

Civil damages for unauthorized inspection or disclosure.

Taxpayer may receive damages of $1000 or actual damage amount

Jail terms up to six months

Unlawful disclosure can result in:

- Misdemeanor or Felony Convictions
- Fines
- Imprisonment
- Civil Actions for Damages
- Agency Disciplinary Actions or Termination

DISCLOSURE

DISCLOSURE OFFICER: DON STAPLES

Liaison between TAX and IRS

DISCLOSURE OFFICER: DON STAPLES

Liaison between TAX and IRS

FEDERAL SAFEGUARD COORDINATOR: CHERYL FOX

Oversees on-going compliance with federal safeguarding requirements

DISCLOSURE OFFICER: DON STAPLES

Liaison between TAX and IRS

FEDERAL SAFEGUARD COORDINATOR: CHERYL FOX

Oversees on-going compliance with federal safeguarding requirements

AGENCY SAFEGUARD ANALYST

Prepares monthly, quarterly and annual reports and assist Federal Safeguard Coordinator with compliance and safeguarding issues

For more detailed descriptions of staff functions, click "**Disclosure Staff Responsibilities**" link in the Attachments tab.

DISCLOSURE OFFICER: DON STAPLES

Liaison between TAX and IRS

FEDERAL SAFEGUARD COORDINATOR: CHERYL FOX

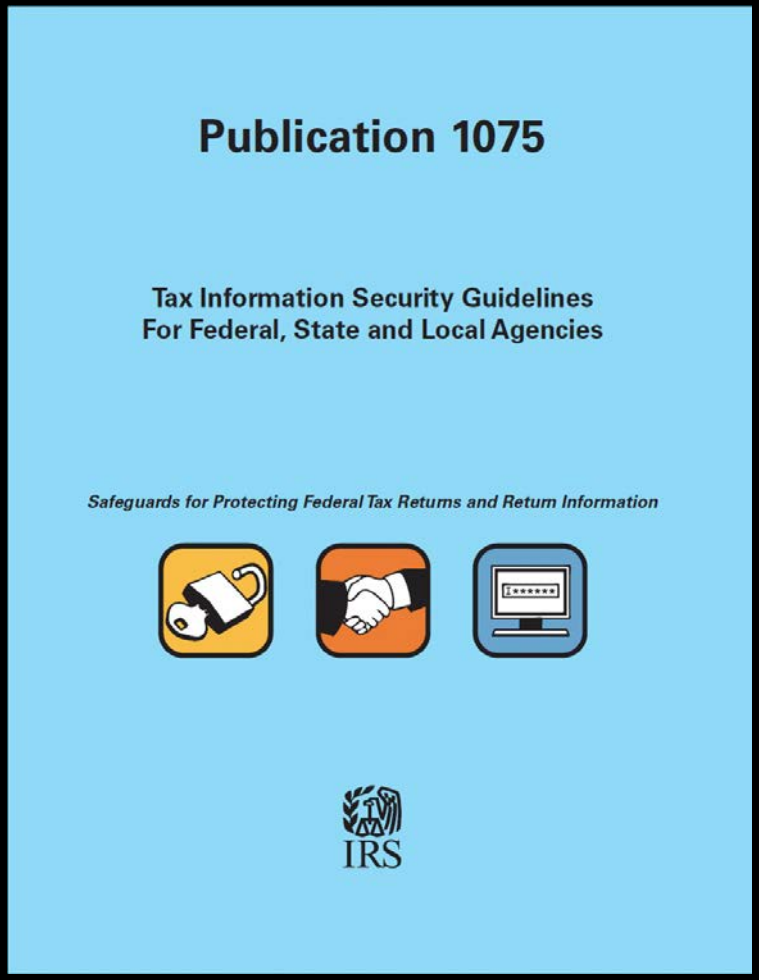
Oversees on-going compliance with federal safeguarding requirements

AGENCY SAFEGUARD ANALYST

Prepares monthly, quarterly and annual reports and assist Federal Safeguard Coordinator with compliance and safeguarding issues

SAFEGUARD SECURITY MANAGER

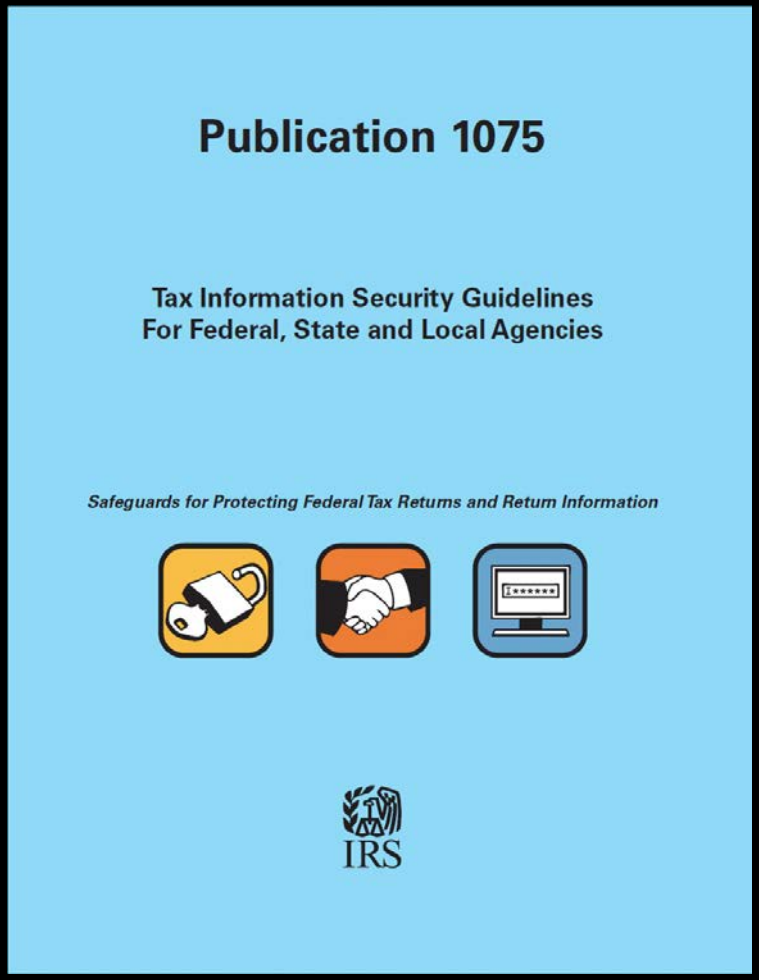
Primary contact between TAX and Virginia Information Technologies Agency (VITA) regarding security of TAX systems



Access

Storage

Destruction



Access

- Job Related
- Need to Know Basis

S.A.F.E.

Screen May Contain Federal Information.

Name

Last: DOE First: JOHN MI:

Title: Suffix:

Customer

SSN: 111-11-1111 Registration Status: Complete

Status: Active Deceased

Primary Address

Street: 111 STREET ST

City: RICHMOND State: Virginia

Zip: 20121-4253 Undeliverable

Save Close

RESTRICTED WORK A

FEDERAL DATA

***** DO NOT ENTER

Unless you have an official need to perform a duties.

In accordance with a signed IRS Agreement, THIS AREA IS RESTRICTED.

Publication 1075

Tax Information Security Guidelines
For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns and Return Information

IRS

Publication 1075

Tax Information Security Guidelines
For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns and Return Information

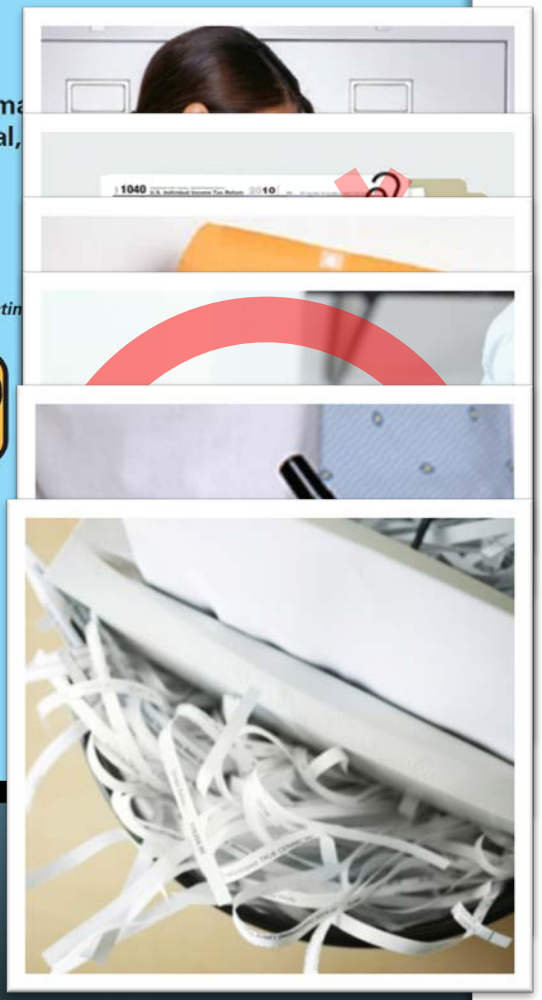
IRS

irs.gov

Publication 1075

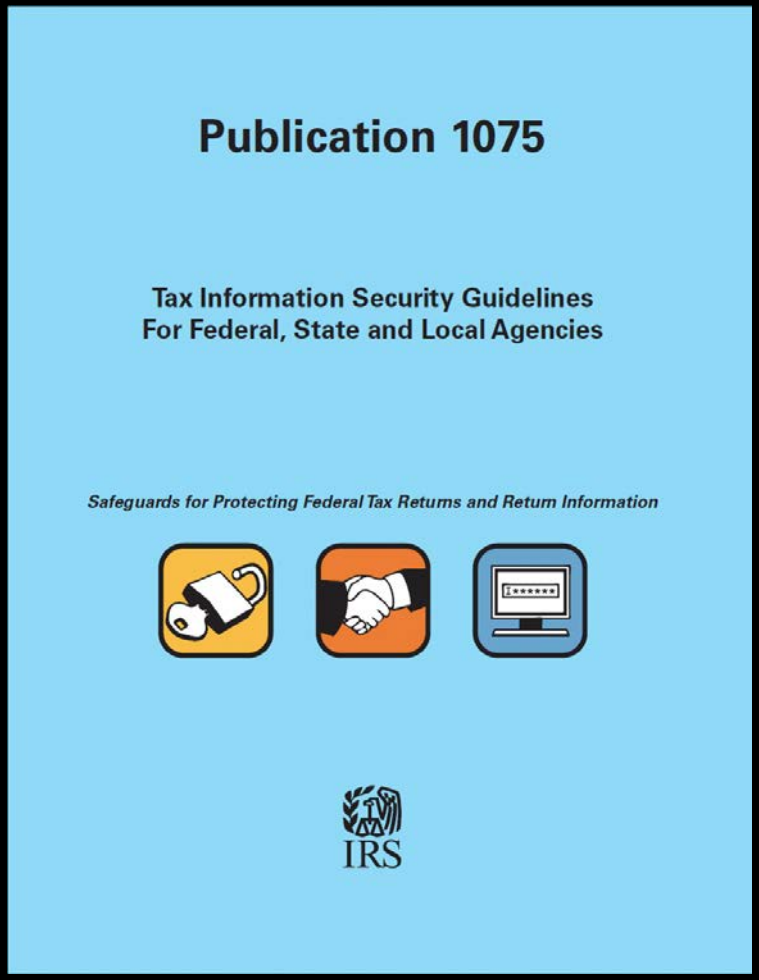
Tax Informa
For Federal,

Safeguards for Protectin



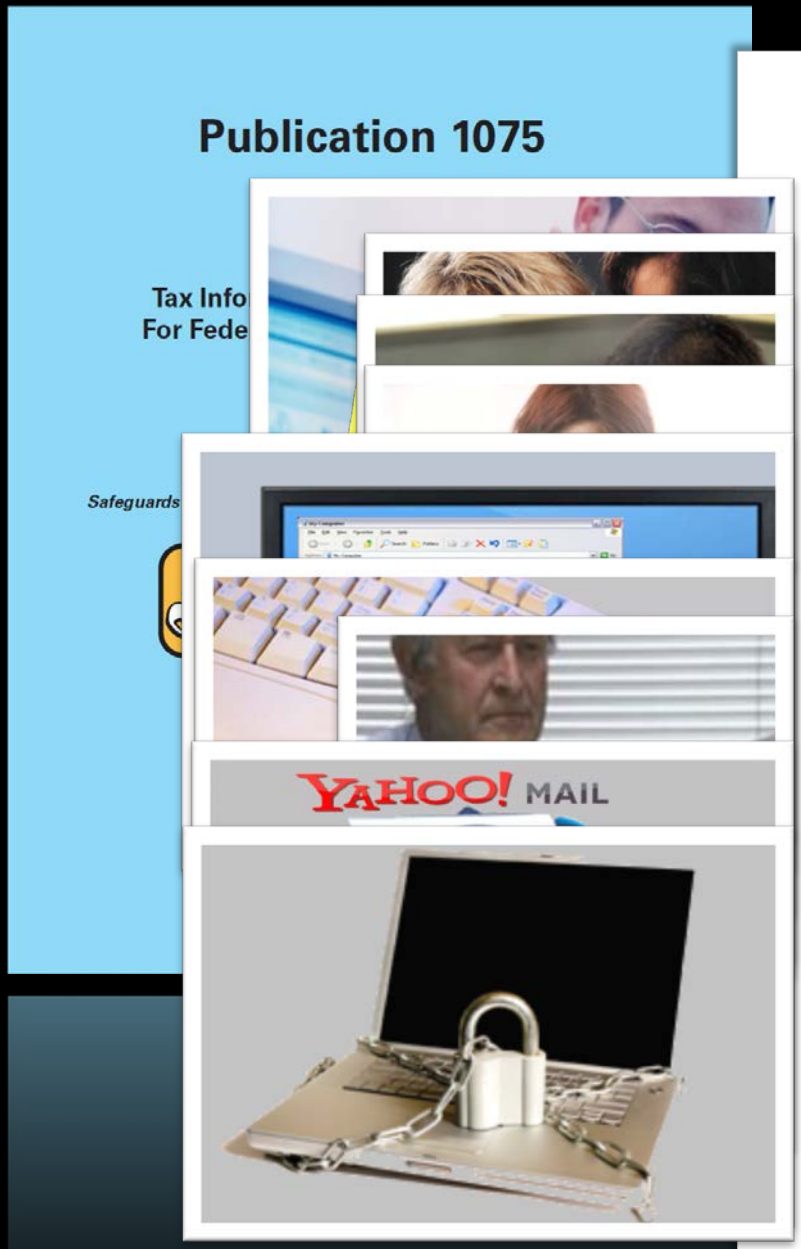
Safeguarding Paper/Hardcopies

- ✓ Secure all federal data in bar-locked cabinets.
- ✓ Ensure no federal taxpayer information is inserted, attached or stapled to files
- ✓ Don’t mail federal tax information with out approval.
- ✓ Never fax federal tax information.
- ✓ Don’t view or store federal tax information at an alternate work location without authorization.
- ✓ Dispose printouts of working papers, spreadsheets, correspondence and notes by shredding or placing in locked destruction containers



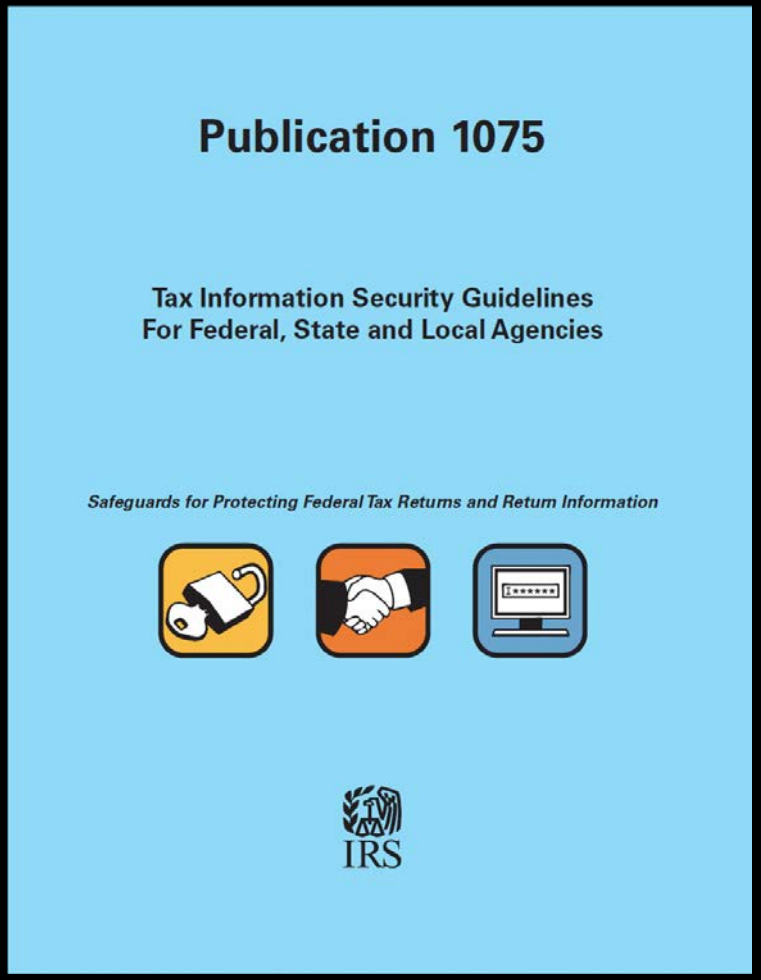
Electronic Media

- IRS Documents
- Federal Data Files
- System Applications
- Working/Test Databases
- Working Electronic Files



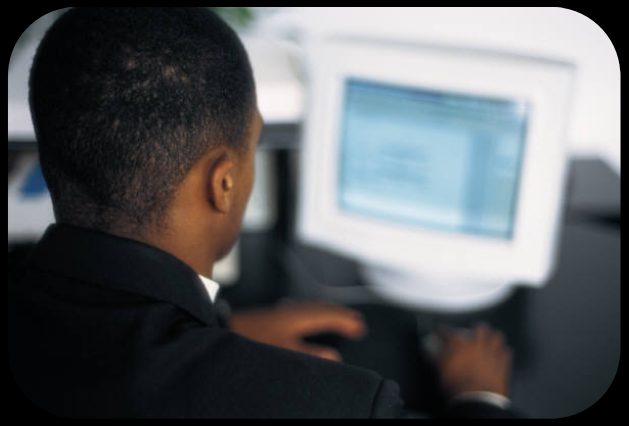
Safeguarding Electronic Data

- ✓ Never leave a workstation unattended
- ✓ Don’t share your password
- ✓ Validate your own access need
- ✓ Ensure staff members you are providing files / screenshots are authorized to access the information
- ✓ Copy federal tax information to approved, secure directories
- ✓ Do not copy federal data to your PC or removable media
- ✓ Consider test data containing federal data or built from production data as confidential
- ✓ Never email federal tax information to an external email address
- ✓ Contact IT Risk Management for guidance or questions for storing electronic data with federal data

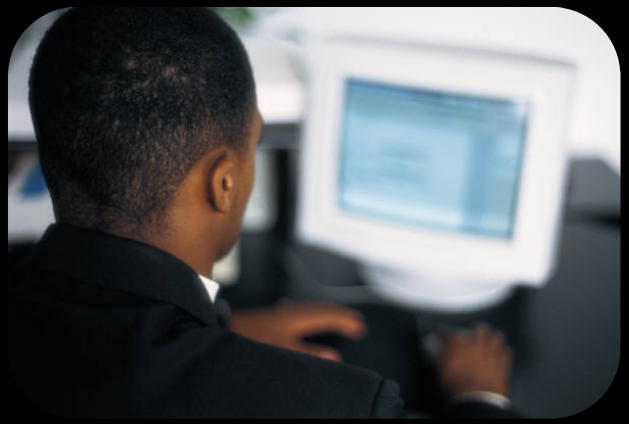


Office Disclosure Guidelines

- Disclosing taxpayer information
- Reporting procedures



Code Authority Procedures



Code Authority Procedures

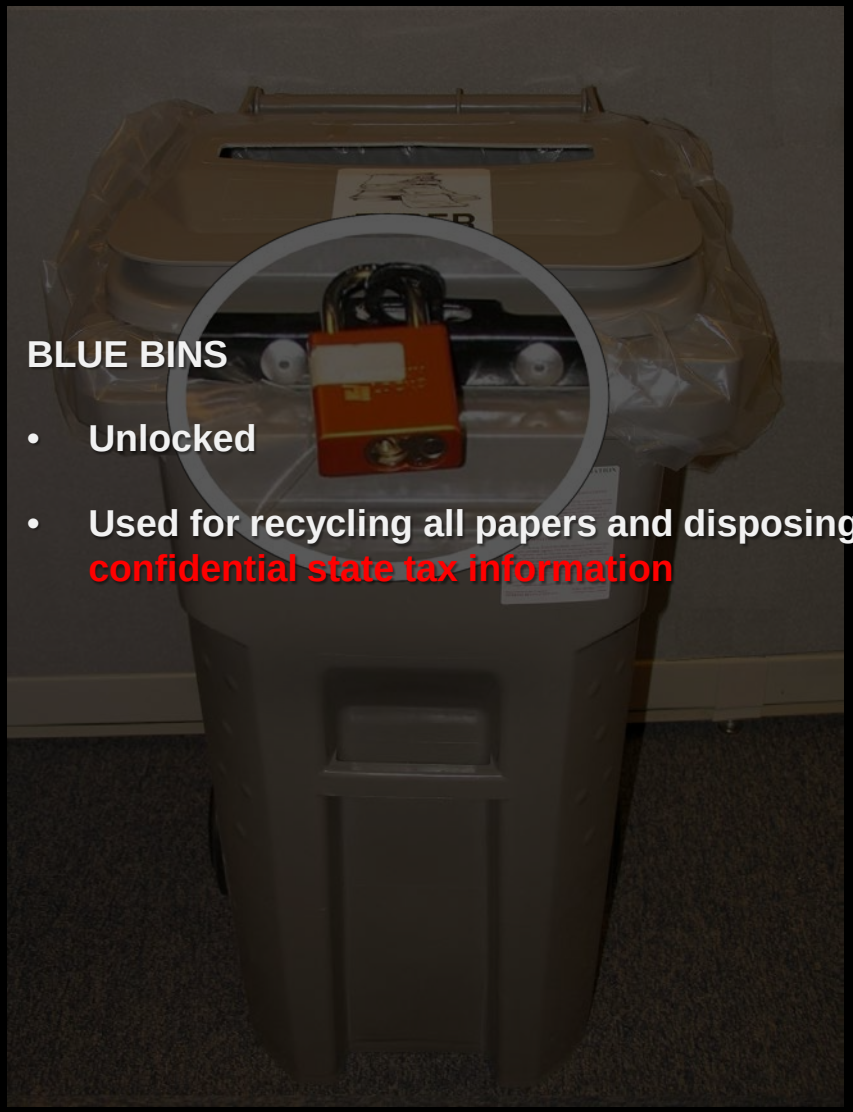
Freedom of Information Act Requests – Public Relations (Joel Davison)

Subpoenas – Customer Service (Shelia Akrie)

Other Disclosure Request – Disclosure Officer (Don Staples)

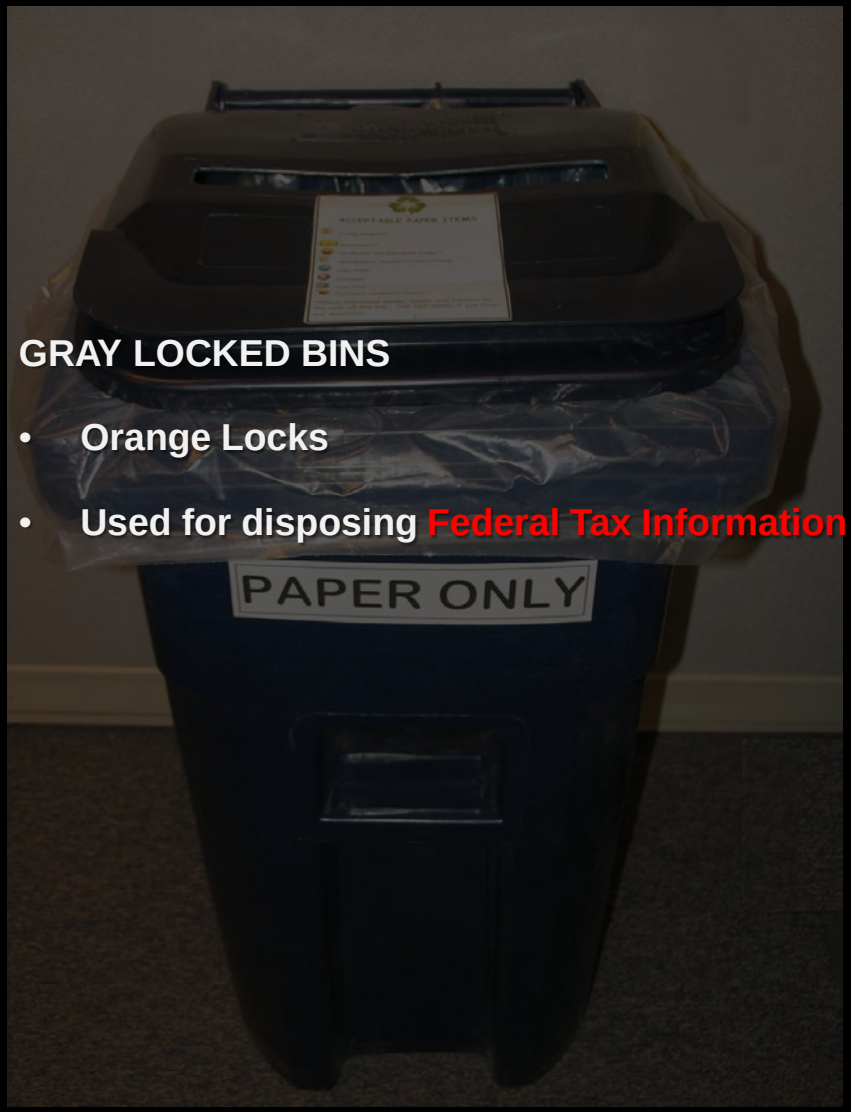
Return all federal transcripts to Office Audit

Deposit spreadsheets, screen prints and correspondence in Federal Tax Information (FTI) witness destruction bins



BLUE BINS

- **Unlocked**
- **Used for recycling all papers and disposing confidential state tax information**



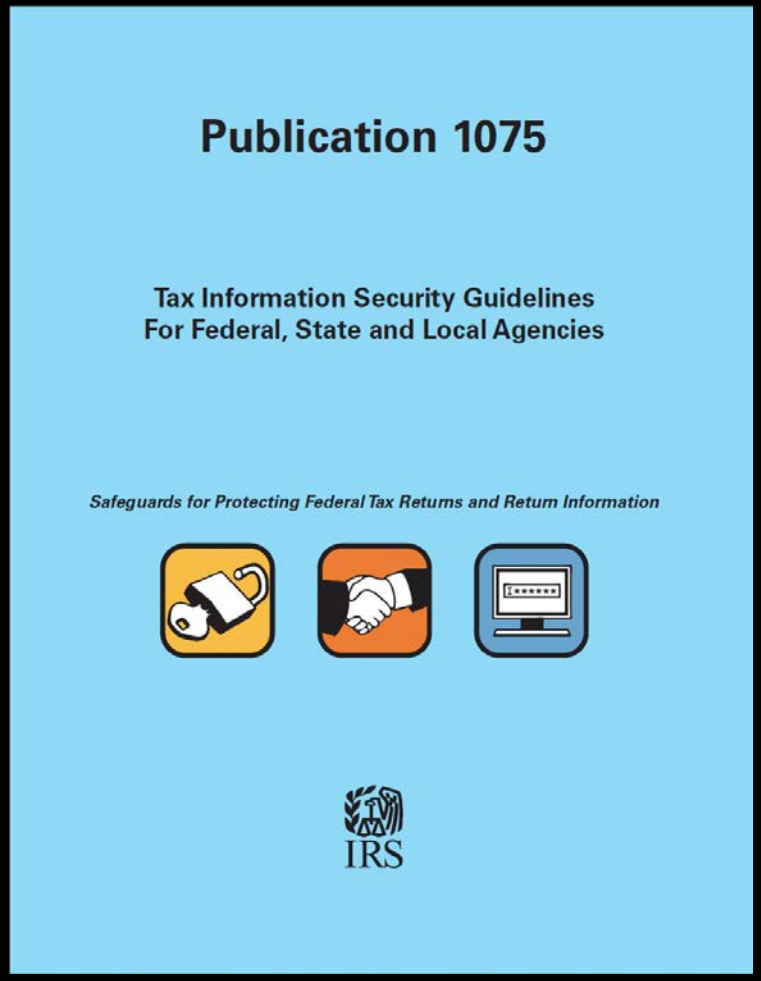
GRAY LOCKED BINS

- **Orange Locks**
- **Used for disposing Federal Tax Information**

Access

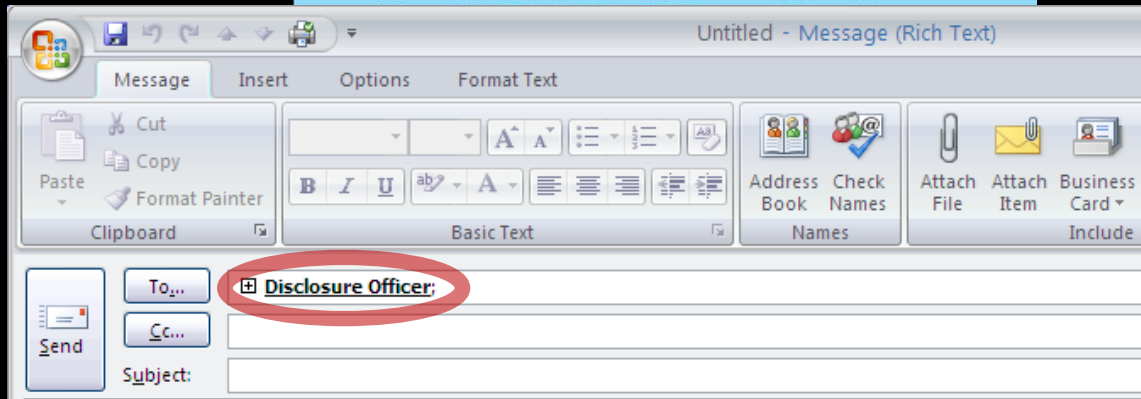
Storage

Destruction



Publication 1075

Tax Information Security Guidelines
For Federal, State and Local Agencies



WHEN was the date of the disclosure

WHAT was the type of information disclosed. *If federal information is involved, describe exactly what was disclosed.*

WHO – disclosed the information

– was the recipient of the disclosed information

HOW was the information disclosed

Internal Audit

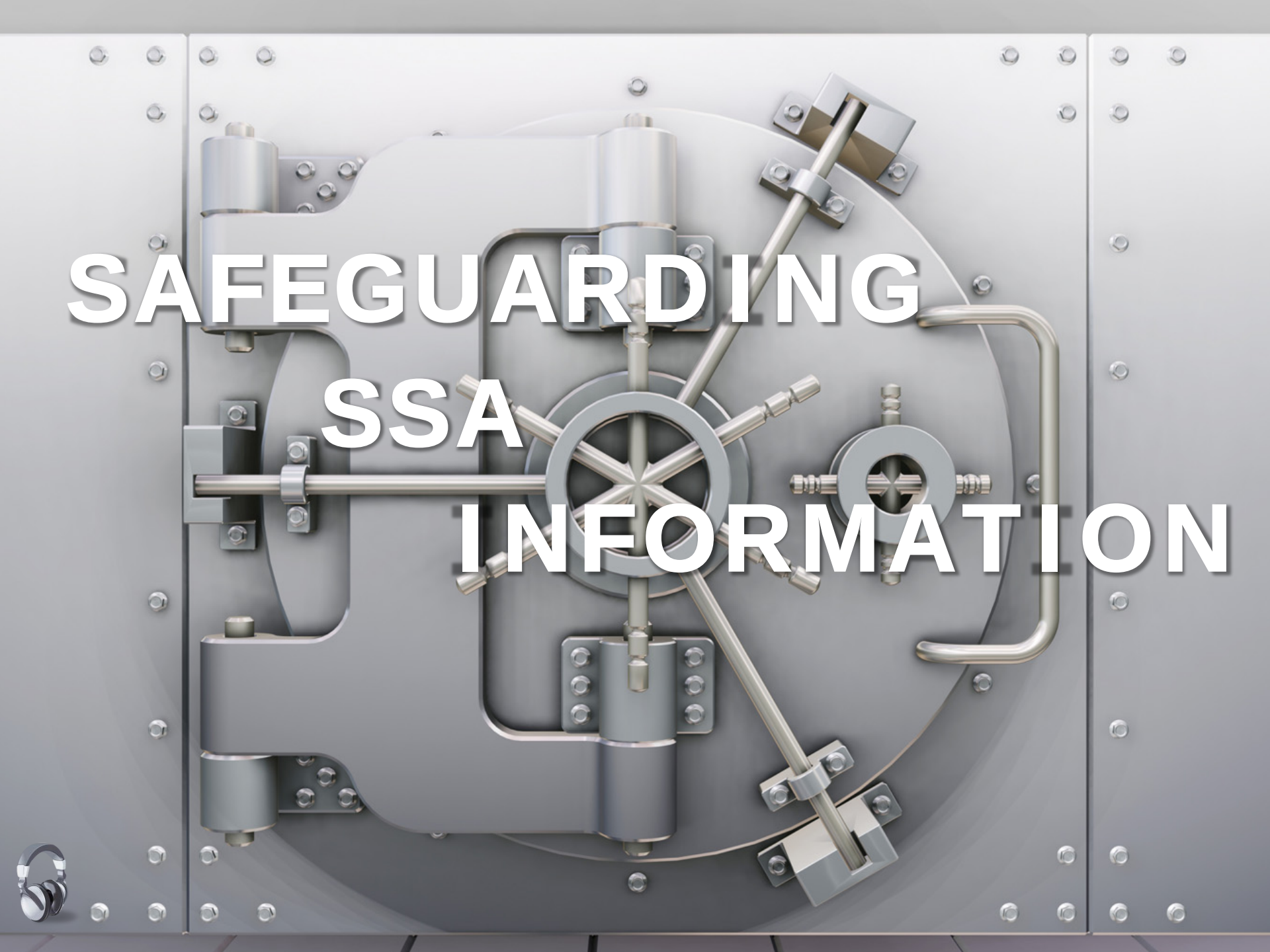
Assistant Commissioner

Human Resources

Supervisor

Federal Safeguard Coordinator

Treasury Inspector General for Tax Administration (TIGTA)


SAFEGUARDING
SSA
INFORMATION

SSA Provided Information

- Similar to the protection of FTI, there are federal standards that are in place that govern and safeguard electronic information provided by the Social Security Agency (SSA).
- TSSRv7 is the document that identifies the requirements in place to meet this objective. These policies and requirements govern our responsibilities of safeguarding and use of SSA provided information.

SSA Provided Information

- The Privacy Act of 1974 is a federal law that governs the collection and use of records maintained about an individual that contains personal identifiers, such as name, social security number, or other identifying number or symbol.
- SEC501 provides additional guidance in the handling and safeguarding of Personally Identifiable Information (PII)

SSA Provided Information

- “Personally Identifiable Information (PII),” covered under several Federal laws and statutes, refers to specific information about an individual used to trace that individual’s identity. Information such as his/her name, Social Security Number (SSN), date and place of birth, mother’s maiden name, or biometric records, alone, or when combined with other personal or identifying information is linkable or lined to a specific individual’s medical, educational, financial, and employment information

SSA Provided Information - Acronyms

- The following Acronyms are used throughout this section.
- TSSR – Technical System Security
- EIEP – Electronic Information Exchange Partners

SSA Provided Information

1. EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP‟s ability to:

   – safeguard the information in conformance with SSA requirements

   – efficiently investigate fraud, data breaches, or security events that involve SSA-provided information

   – detect instances of misuse or abuse of SSA-provided information

SSA Provided Information

1. The EIEP must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
2. The EIEP must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
3. The EIEP must use the software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA
4. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.
5. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.

SSA Provided Information

6. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

   NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP.

7. EIEPs must store information received from SSA in a manner that, at all times, is physically and electronically secure from access by unauthorized persons.
8. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.
9. EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.

SSA Provided Information

10. EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided.
11. EIEPs must have an active and robust security awareness program, which is mandatory for all employees who access SSA-provided information. Training shall include:
    a) The security awareness should include the sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse.
    b) The rules of behavior concerning use and security in systems and/or applications processing SSA-provided information.
    c) The restrictions on viewing and/or copying SSA-provided information
    d) The responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA-provided information.
    e) The proper disposal of SSA-provided information.
    f) The security breach and data loss incident reporting procedures.
    g) The basic understanding of procedures to protect the network from malware attacks.

SSA Provided Information

h) Spoofing, phishing and pharming and network fraud prevention.
i) The possible criminal and civil sanctions and penalties for misuse of SSA-provided information

12. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained.
13. In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency plan that includes a disaster recovery plan that addresses both natural disaster and cyber-attack situations.

SSA Provided Information

14. SSA requires the Contingency Plan to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs.
15. At its discretion, SSA or its designee must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.
16. The EIEP must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP's ability to:
    a) Safeguard the information in conformance with SSA requirements.
    b) Efficiently investigate fraud, data breaches, or security events that involve SSA-provided information.
    c) Detect instances of misuse or abuse of SSA-provided information.

SSA Provided Information

17. The EIEP must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.
18. The EIEP must use an Intrusion Prevention Protection System (IPS) or an Intrusion Detection System (IDS) and provide continuous monitoring of its network infrastructure and assets to ensure that:
    a) The EIEP's security controls continue to be effective over time.
    b) The EIEP uses industry-standard Security Information Event Manager (SIEM) tools, anti-malware software, and effective antivirus protection.
    c) Only authorized individuals, devices, and processes have access to SSA-provided information.
    d) The EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions as soon as they occur.
    e) The necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes.

SSA Provided Information

f) Upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk.
g) In the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions.
h) Trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible.

19. The EIEP must employ measures to ensure that communications and data furnished to SSA contain no viruses or other malware.
20. The EIEP must have procedures in place to ensure the proper methods of media sanitization.
    a) Disposal: Refers to the discarding (e.g., recycling) media that contains no sensitive or confidential data.

SSA Provided Information

b) Overwriting/Clearing: This type of media sanitization is adequate for protecting information from a robust keyboard attack. Clearing must prevent retrieval of information by data, disk, or file recovery utilities. Clearing must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. Deleting items, however, is not sufficient for clearing. This process may include overwriting all addressable locations of the data, as well as its logical storage location (e.g., its file allocation table). The aim of the overwriting process is to replace or obfuscate existing information with random data. Most rewriteable media may be cleared by a single overwrite. This method of sanitization is not possible on un-writeable or damaged media.

c) Purging: This type of media sanitization is a process that protects information from a laboratory attack. The terms *clearing* and *purging* are sometimes synonymous. However, for some media, clearing is not sufficient for purging (i.e., protecting data from a laboratory attack). Although most re-writeable media requires a single overwrite, purging may require multiple rewrites using different characters for each write cycle. This is because laboratory attack involves threats with the capability to employ non-standard assets (e.g., specialized hardware) to attempt data recovery on media outside of that media's normal operating environment.

d) Degaussing is also an example of an acceptable method for purging magnetic data. The EIEP should destroy media if purging is not a viable method of sanitization.

SSA Provided Information

e) Destruction: Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual media should be able to withstand laboratory attack.

SSA Provided Information

- *If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact* ***within one hour****, the responsible State Agency official or delegate must report the incident by contacting* ***SSA's National Network Service Center (NNSC) toll free at 877-697-4889*** *(select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

SSA Provided Information

Similar to FTI data, the misuse or unauthorized disclosure of SSA-provided information can result in potential criminal and/or civil sanctions or penalties.

For a printed copy of this lesson, click the "**Lesson Transcript**" link in the Attachments tab.

SOURCES

DISCLOSURE

SAFEGUARDING