



# IRS SECURITY OF TAXPAYER INFORMATION: CHARACTERISTICS OF EMPLOYEE UNAUTHORIZED ACCESS AND DISCLOSURE CASES

May 2022

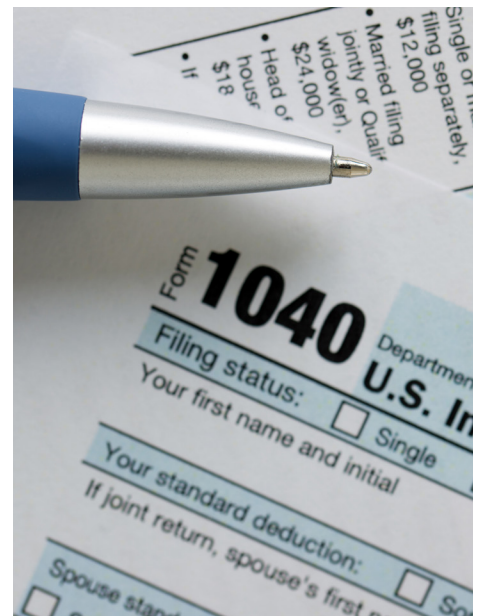
Our tax system—administered by the Internal Revenue Service (IRS)—is based largely on voluntary compliance. One factor that may influence voluntary compliance includes whether taxpayers feel confident that the personal and financial information they provide IRS is properly safeguarded.

Federal tax information consists of federal tax returns and return information that is in IRS’s possession or control and is covered by confidentiality protections and safeguards in section 6103 of the Internal Revenue Code.<sup>1</sup> The code defines and protects the confidentiality of information taxpayers provide to IRS and criminalizes certain violations of this confidentiality.

The willful unauthorized inspection of taxpayer returns or return information by employees and contractors authorized to receive federal taxpayer information is a crime.<sup>2</sup> The willful unauthorized disclosure of a taxpayer’s return or return information is also a crime.<sup>3</sup>

Recent news reported on tax return information and stated that the news organization had a large amount of IRS tax data on certain types of taxpayers.<sup>4</sup> In light of this, you asked us to review IRS’s policies for protecting tax information.

**FIGURE 1: INTERNAL REVENUE SERVICE INDIVIDUAL TAX RETURN**



Source: Stock.Adobe.com/Kenishirotie. | GAO-22-105872

<sup>1</sup>26 U.S.C. § 6103. These confidentiality protections and safeguards continue to apply when IRS shares federal tax information with other entities, such as other federal or state agencies, pursuant to section 6103.

<sup>2</sup>26 U.S.C. § 7213A.

<sup>3</sup>26 U.S.C. § 7213.

<sup>4</sup>ProPublica, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax* (June 8, 2021).

This report describes IRS's processes for safeguarding federal tax information as well as what is known about cases of willful unauthorized access, attempted access, or inspection of federal tax information (UNAX) and unauthorized disclosure of federal tax information by IRS employees, with the exception of IRS Chief Counsel employees.<sup>5</sup> Our report is presented in a question-and-answer format. The first half of the questions describe IRS's processes for safeguarding federal tax information. Our analysis of what is known about cases of UNAX and unauthorized disclosure by IRS employees follows that part.

To describe IRS's processes for safeguarding federal tax information, we reviewed relevant statutes and IRS documentation to understand IRS's protections of federal tax information, who is allowed to access and disclose federal tax information, the circumstances under which access and disclosure is allowed, and the potential penalties for accessing and disclosing this information inappropriately. Specifically, we reviewed relevant sections of the Internal Revenue Code, the *Internal Revenue Manual*, and IRS's *Manager's Guide to Penalty Determination*.<sup>6</sup>

We also reviewed IRS and Treasury Inspector General for Tax Administration (TIGTA) documentation. In addition, we interviewed knowledgeable IRS and TIGTA officials to understand the process for reporting and investigating unconfirmed instances of UNAX or unauthorized disclosure.

To describe the characteristics of cases of UNAX and unauthorized disclosure, we analyzed data from IRS on employee misconduct cases that TIGTA sent to IRS between fiscal years 2012 and 2021.<sup>7</sup> We chose this time period because it was the most recent 10-year time period. We identified cases in this dataset that were marked with a UNAX issue code.<sup>8</sup> From there, we identified cases that had also been classified with a disclosure issue code to be further investigated for federal tax information disclosure. We analyzed UNAX cases that also had a disclosure issue included as part of that case, but this report does not contain a comprehensive analysis of unauthorized disclosure of federal tax information by IRS employees.<sup>9</sup> We also reviewed

<sup>5</sup>IRS Chief Counsel employees comprised about 3 percent of the overall IRS workforce in fiscal year 2021. IRS Chief Counsel employees are not covered in this analysis because that office uses a separate system to track UNAX and unauthorized disclosures of federal tax information. Our report also does not include UNAX and unauthorized disclosure violations committed by IRS contractors or others permitted to access federal tax information (e.g., local, state, or other federal government employees). We have ongoing work reviewing IRS's controls to protect federal tax information. As part of that work, we are reviewing IRS's policies and data related to IRS contractor UNAX. We did not review IRS's Office of Safeguards, which manages access to federal tax information for local, state, and other federal government employees, because this office reviews our tax data safeguards.

<sup>6</sup>26 U.S.C. §§ 6103, 7213, 7213A, 7431; Internal Revenue Service, *Internal Revenue Manual*, §§ 1.1.12, 10.5.1, 10.5.5; Internal Revenue Service, *Manager's Guide to Penalty Determinations*, Document 11500 (August 2012).

<sup>7</sup>Our analysis is based on IRS employee UNAX cases. We did not analyze characteristics of cases where IRS investigated employees for lesser unauthorized access or disclosure issues, such as inadvertent or negligent unauthorized access or disclosure. This case information is stored in IRS's Automated Labor and Employee Relations Tracking System that tracks labor and employee relations case data.

<sup>8</sup>Issue codes identify relevant case issues investigated as part of a case (e.g., loss of government cell phone, UNAX, purchase card misuse). We did not review TIGTA's classification of cases as UNAX. According to IRS officials, in some instances, they did not view these TIGTA-referred cases as UNAX cases. It is also possible that IRS added a UNAX issue to cases that originated from TIGTA after investigating other issues.

<sup>9</sup>Because the code that identifies a case that has a disclosure issue is not specific to disclosure of federal tax information, we could not use this code to comprehensively identify employee misconduct cases related to unauthorized disclosure of federal tax information. This code can be used in instances where other sensitive information, such as personally identifiable information, is disclosed without authorization or for instances when office security is compromised. Based on our discussions with knowledgeable IRS officials, we classified cases with both a disclosure and a UNAX issue code as cases where the disclosure issue was related to the unauthorized disclosure of federal tax information. We did not manually review case details for these cases due to the confidentiality protections of federal tax information. In addition, we could not identify whether other disclosure cases were related to the unauthorized disclosure of federal tax information.

IRS documentation and interviewed knowledgeable IRS officials to understand data definitions and for context.

We determined IRS's data were sufficiently reliable to describe the characteristics of IRS employee cases.<sup>10</sup> To assess data reliability, we reviewed IRS documentation and interviewed knowledgeable IRS officials. We also compared our calculations of cases closed by fiscal year to IRS's internal documentation of such cases to ensure consistency. Additionally, we conducted testing to identify missing values and obvious outliers and errors.

We conducted this performance audit from August 2021 to May 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# QUESTIONS AND ANSWERS ON IRS SECURITY OF TAXPAYER INFORMATION

## WHAT IS FEDERAL TAX INFORMATION?

Federal tax information consists of federal tax returns and return information (and information derived from it) that is in IRS's possession or control and is covered by the confidentiality protections of the Internal Revenue Code. This includes returns or return information received directly by IRS or obtained through an authorized secondary source such as the Social Security Administration or another entity acting on IRS's behalf.

**Returns.** A return is any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the Internal Revenue Code and filed with IRS by, on behalf of, or with respect to any person or entity.

**Return information.** Return information, in general, is any information collected or generated by IRS regarding any person's tax liability or possible liability.<sup>11</sup> For example, return information includes information extracted from a return, including names of dependents or the location of a business and the status of whether a return was filed.

In certain circumstances, IRS is permitted to disclose federal tax information to other entities, such as federal, state, and local agencies. For example, according to IRS documentation, IRS shares federal tax

<sup>10</sup>We did not assess IRS's case determinations.

<sup>11</sup>Return information also includes any advance pricing or closing agreement and related background information entered into by IRS and the taxpayer. 26 U.S.C. § 6103(b)(2).

information with state tax agencies to improve tax administration by reducing duplicate government resource expenditures and increasing taxpayer compliance.<sup>12</sup> In these instances, the shared information is still considered federal tax information and protected as such. As a condition of receiving this information, the receiving agency must demonstrate, to the satisfaction of IRS, the ability to protect its confidentiality.

## HOW DOES IRS PROTECT FEDERAL TAX INFORMATION?

IRS's Privacy, Governmental Liaison and Disclosure (PGLD) and Information Technology Cybersecurity offices both oversee policies and practices that protect sensitive information, including federal tax information. PGLD oversees IRS privacy and records management policies, coordinates privacy protection guidance and activities, responds to privacy complaints, and promotes data protection awareness throughout IRS. As part of this work, PGLD develops policies, standards and guidelines related to disclosure of information, including federal tax information. PGLD also creates agency-wide privacy training materials and communications pertaining to privacy requirements. For example, PGLD could provide employees with notices about being aware of their home surroundings while teleworking (e.g., what smart devices with built-in digital assistants are listening to them).

PGLD also oversees IRS's UNAX Program. The UNAX Program's mission is to ensure all IRS employees and contractors (1) understand what UNAX is; (2) understand the consequences of accessing or inspecting tax information for other than management authorized tax administration reasons; and (3) work to prevent UNAX violations. In this capacity, the program produces educational materials, including an annual security of taxpayer information briefing aimed at preventing and reducing the number of UNAX incidents.

The Cybersecurity office is responsible for protecting IRS's systems, services, and data, including taxpayer information, from internal and external cyber-related threats.<sup>13</sup> The office also conducts auditing and monitoring activities and provides protection of sensitive but unclassified data, including taxpayer information.<sup>14</sup>

## WHAT ARE IRS EMPLOYEE RESPONSIBILITIES WHEN ACCESSING AND DISCLOSING FEDERAL TAX INFORMATION?

IRS employees are responsible for accessing IRS paper or electronic tax returns or tax return information only when it is required to complete official IRS duties as assigned. Further, IRS employees are responsible for protecting the confidentiality and privacy of taxpayer information to which they have access.

If IRS employees access tax information that (1) is not a part of their assigned duties, or (2) is otherwise prohibited, then this access

<sup>12</sup>See 26 U.S.C. § 6103(d).

<sup>13</sup>See Internal Revenue Service, *Internal Revenue Manual* § 1.1.12.3, ACIO for Cybersecurity (Feb. 24, 2021).

<sup>14</sup>According to IRS officials, the Cybersecurity office provides audit and monitoring capabilities to systems that the IRS Information Technology organization maintains.

### Investigation Terminology

- **Incident:** Investigations begin with an incident, an unconfirmed instance of suspected willful unauthorized access or disclosure. Incidents are reported to the Treasury Inspector General for Tax Administration (TIGTA) for investigation.

- **Case:** Once under investigation, an incident becomes part of a case as it is investigated by TIGTA and, subsequently, IRS. A closed case is an investigation that has been completed by both TIGTA and IRS.

- **Violation:** A case is considered to be substantiated as a willful unauthorized access or disclosure violation after IRS confirms an employee willfully accessed federal tax information that was not part of the employee's assigned duties or was prohibited or willfully disclosed tax information to someone without authorization to have this information, respectively. Violations can be referred to as substantiated cases.

Source: GAO analysis of Internal Revenue Service (IRS) and TIGTA information. | GAO-22-105872

## HOW ARE CASES OF UNAUTHORIZED ACCESS AND DISCLOSURE INVESTIGATED?

is unauthorized.<sup>15</sup> Unauthorized access can either be considered inadvertent—performed in error—or UNAX—the willful unauthorized access, attempted access, or inspection of tax returns or return information. One type of inadvertent access can occur when an IRS employee accidentally enters an incorrect Taxpayer Identification Number.

According to the *Internal Revenue Manual*, IRS officials are only to disclose tax information if there is a statutory basis that allows the disclosure, the proper authorization to disclose this information has been granted, and written procedures for making the disclosure exist.<sup>16</sup> IRS considers a number of factors including the authentication of the intended recipient and the recipient's need to know when deciding to disclose taxpayer information.

Similar to unauthorized access, disclosures of tax information that are not authorized can be considered inadvertent or willful. Inadvertent disclosures are unintended, whereas willful unauthorized disclosures, or what we are referring to as unauthorized disclosure, are intentional.

Instances of suspected UNAX or unauthorized disclosure are described as incidents. They are investigated as cases to determine whether or not the incident can be substantiated, or that a violation occurred.<sup>17</sup>

TIGTA investigates IRS programs and operations. As part of that responsibility, it also investigates UNAX and unauthorized disclosure cases.<sup>18</sup> TIGTA's Office of Investigations evaluates cases to determine if UNAX or unauthorized disclosure incidents warrant investigation.

As shown in figure 2, TIGTA becomes aware of UNAX and unauthorized disclosure incidents when someone reports an incident or through its own analysis of IRS reports, both of which can originate from a number of sources.

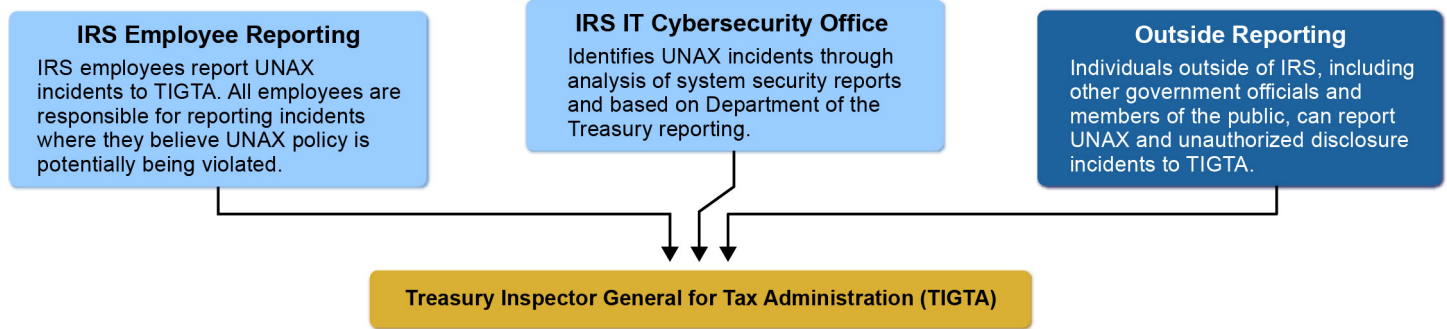
<sup>15</sup>IRS employees are not authorized to access the tax records or tax information of anyone with whom they have a covered relationship, including their spouse and any ex-spouses; their children; their parents and grandparents; anyone living in their household; their other close relatives; friends or neighbors with whom they have close relationships; celebrities, when the information is not needed to carry out tax-related duties; an individual or organization for which they or their spouse is an officer, trustee, general partner, agent, attorney, consultant, contractor, employee, or member; and any other individual or organization with whom they may have a personal or outside business relationship that could raise questions about their lack of impartiality in handling the tax matter. Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.5(1) Covered Relationships (July 10, 2018).

<sup>16</sup>Internal Revenue Service, *Internal Revenue Manual* § 11.3.1.2(2) Disclosure Code, Authority and Procedure (CAP) (Mar. 13, 2018).

<sup>17</sup>IRS's inability to substantiate a violation does not necessarily mean that an employee did not commit a UNAX or unauthorized disclosure violation, but that IRS was unable to find proof that the violation occurred.

<sup>18</sup>Department of the Treasury, *Office of the Treasury Inspector General for Tax Administration*, Treasury Order 115-01 (May 24, 2018).

FIGURE 2: INCIDENT REPORTING TO TIGTA



Sources: GAO analysis of Internal Revenue Service (IRS) and TIGTA information. | GAO-22-105872

Note: UNAX is the willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.

**IRS employee reporting.** According to the *Internal Revenue Manual*, IRS employees are required to report all incidents to TIGTA for investigation.<sup>19</sup>

**IRS Cybersecurity office reporting.** The Cybersecurity office analyzes system security reports obtained from IRS's Security Audit and Analysis System that display employees' accesses of federal tax information.<sup>20</sup> The office then partners with IRS management to determine the validity of these accesses. The Security Audit and Analysis System is a centralized data repository that collects audit logs from various applications. It collects and processes information necessary for IRS and TIGTA to detect potential unauthorized accesses to IRS systems and data and to reconstruct events for potential criminal investigations. The Cybersecurity office subsequently refers any incidents to TIGTA for investigation. According to IRS officials, the Cybersecurity office also becomes aware of incidents from the Department of the Treasury. When Treasury notifies the Cybersecurity office of an incident, the office is to perform analysis and, if appropriate, refer it to TIGTA.

**Outside reporting.** Other government personnel and private citizens can report incidents to TIGTA.

TIGTA evaluates referrals to determine if the UNAX or unauthorized disclosure incidents warrant investigation. According to a TIGTA official, it also identifies UNAX incidents by analyzing system security reports that it obtains from IRS's Security Audit and Analysis System. TIGTA officials further explained that TIGTA has a dedicated group that performs in-depth analysis of employee access to taxpayer accounts to proactively identify UNAX incidents. This could include analyzing IRS employee behavior to determine whether access was inadvertent or needs to be further investigated.

<sup>19</sup>See Internal Revenue Service, *Internal Revenue Manual* § 10.5.5.3.4(10) Employee and Contractor UNAX Responsibilities (July 10, 2018).

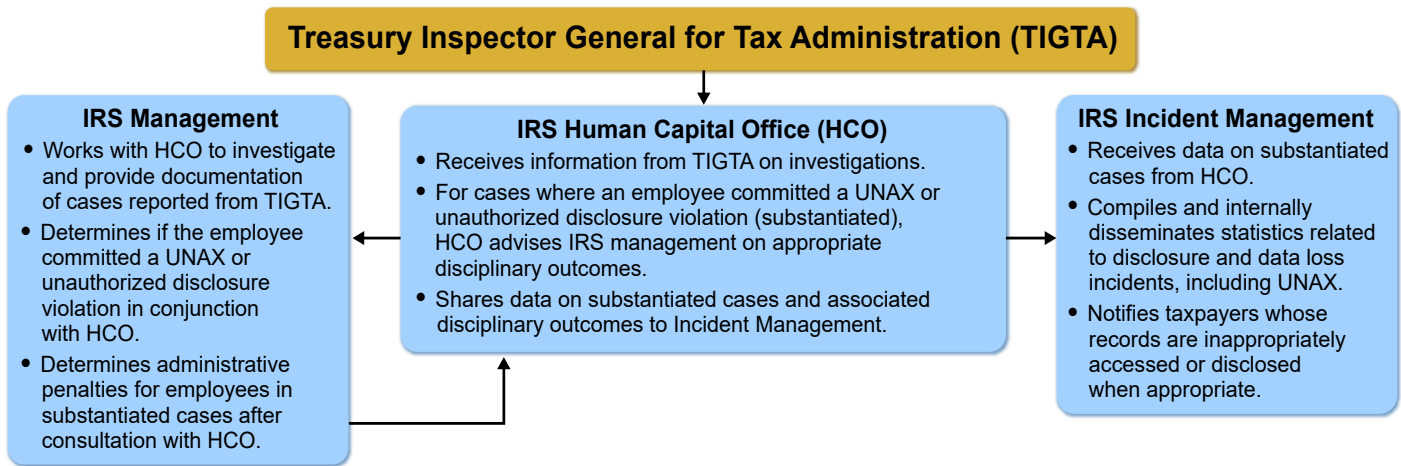
<sup>20</sup>All modernized IRS systems containing taxpayer data are required to send their system and program transactions (audit logs) to the Security Audit and Analysis System.

If a UNAX or unauthorized disclosure incident warrants investigation, officials take several steps to investigate. These steps include interviewing UNAX victims, interviewing the investigated employee’s supervisor, and reviewing reports of the employee’s accesses to tax information, as appropriate. According to IRS officials, TIGTA may ask the IRS Cybersecurity office to perform monitoring for UNAX and transfer any collected information to TIGTA.

If TIGTA determines there is sufficient evidence to suggest a UNAX or unauthorized disclosure violation occurred, officials refer the case to the Department of Justice to determine if it would like to pursue prosecution. According to TIGTA officials, between fiscal years 2012 and 2021, the Department of Justice accepted 35 of 2,043 TIGTA referrals for prosecution involving employee UNAX or unauthorized disclosure.

Next, as shown in figure 3, TIGTA provides IRS with the information it collected during its investigation. According to a TIGTA official, the report of investigation is an independent account and does not determine whether an incident was substantiated.

**FIGURE 3: IRS UNAX AND UNAUTHORIZED DISCLOSURE CASE INVESTIGATION AND PENALTY DETERMINATION PROCESS**



Sources: GAO analysis of Internal Revenue Service (IRS) and TIGTA information. | GAO-22-105872

Notes: UNAX is the willful unauthorized access, attempted access, or inspection of taxpayer returns or return information. IRS’s Human Capital Office does not receive data on IRS Chief Counsel employee UNAX cases. TIGTA refers these directly to the IRS Chief Counsel office. These cases are not included in this graphic. After IRS determines a final action for a substantiated UNAX case, offending employees have 30 to 45 days to file an appeal, depending on the appeals process.

Once IRS receives this information, IRS’s Human Capital Office oversees and supports IRS’s investigation process for UNAX and unauthorized disclosure cases. Specifically, this office tracks cases in IRS’s employee misconduct case database, forwards case evidence to the management chain of the employee being investigated, and provides advice and guidance to management as they determine the

final disposition of the penalty. To investigate, track, and determine the penalty outcomes of cases, the IRS Human Capital Office works with the manager and supervisory chain of the employee being investigated.

## HOW ARE UNAUTHORIZED ACCESS AND DISCLOSURE VIOLATIONS PENALIZED?

For cases that IRS determines warrant disciplinary action, the employee's management team determines the appropriate penalties.<sup>21</sup> Managers are to consider the facts of the case, as well as aggravating and mitigating factors.<sup>22</sup> However, IRS policy generally requires removal of the IRS employee to be proposed for all UNAX violations.<sup>23</sup> IRS policy also states that removal is an appropriate penalty for willful unauthorized disclosure violations.

Some cases have multiple issues and managers determine penalties for the totality of the case. For example, a case where IRS management substantiates a UNAX issue as well as a separate issue will result in one overall penalty. These penalties include, but are not limited to, removal or suspension of the employee.

IRS employees convicted of criminal UNAX or unauthorized disclosure violations can face jail time, as well as fines.<sup>24</sup> Criminal unauthorized access violations are punishable by a fine not to exceed \$1,000 or imprisonment of not more than 1 year, or both, together with the costs of prosecution. Upon conviction, the employee is terminated.<sup>25</sup> The willful unauthorized disclosure of tax return or return information is a felony, punishable by a fine of up to \$5,000, up to 5 years in jail, or both, plus costs of prosecution.<sup>26</sup>

IRS is required to notify taxpayers whose information was accessed if the agency proposed disciplinary or adverse action against an employee for unauthorized access or disclosure. Also, these taxpayers can bring civil action to seek damages.<sup>27</sup> This notice includes the date of the unauthorized access or disclosure and information on taxpayer rights. If the offending IRS employee is found liable for disclosing tax information, the federal government may face damages of \$1,000 per unauthorized access or disclosure.

After an investigation, if IRS determines a penalty is warranted, investigated IRS employees can appeal these penalties through different

<sup>21</sup>According to IRS's *Manager's Guide to Penalty Determinations*, each business unit determines the level of supervisory authority required for taking disciplinary or adverse actions. According to IRS officials, each business unit may develop their own delegation orders—documentation that determines the appropriate supervisory level of the management official who can take the action—but these orders must be in compliance with IRS-wide delegation policy.

<sup>22</sup>Deciding officials are required to consider a set of factors known as the Douglas Factors when determining the appropriate penalty for misconduct for bargaining unit employees or when considering adverse actions (e.g., suspensions, removal, reduction in grade or pay, furlough of 30 days or less of a full-time employee). These factors include, among other things, prior disciplinary actions, performance, and potential for rehabilitation. *Douglas v. Veterans Administration*, 5 M.S.P.R. 280 (1981); Internal Revenue Service, *Internal Revenue Manual* § 6.751.1.6(3) Progressive Discipline (Nov. 4, 2008).

<sup>23</sup>The IRS penalty guide provides a range of penalties, including suspension and removal. Management reviews the facts and circumstances of the case to determine the appropriate penalty. Internal Revenue Service, *Manager's Guide to Penalty Determinations*, Document 11500 (August 2012).

<sup>24</sup>26 U.S.C. §§ 7213, 7213A. Former IRS employees and others permitted access to federal tax information (e.g., state and other federal employees) can also be prosecuted for unauthorized access and unauthorized disclosure and face these penalties.

<sup>25</sup>26 U.S.C. § 7213A(b).

<sup>26</sup>26 U.S.C. § 7213(a).

<sup>27</sup>26 U.S.C. § 7431.



processes. Specifically, IRS employees can appeal these decisions through IRS's Equal Employment Opportunity complaint process, arbitration, or the Merit Systems Protection Board, depending on the final action.<sup>28</sup> According to the IRS collective bargaining agreement with the National Treasury Employees Union, at the time IRS issues its proposal and decision letters to an employee, the agency is to include information on employee appeal rights. IRS employees have 30 to 45 days to appeal IRS's final decision, depending on which process they choose. If IRS's final decision includes certain adverse actions against an employee, the employee may appeal the decision to the Merit Systems Protection Board.<sup>29</sup>

### HOW MANY CASES OF UNAUTHORIZED ACCESS AND DISCLOSURE BY IRS EMPLOYEES WERE INVESTIGATED IN RECENT YEARS?

Between fiscal years 2012 and 2021, IRS investigated more than 1,700 employee misconduct cases that included a UNAX issue. TIGTA referred these cases to IRS and they generally represent all UNAX incidents involving IRS employees over the 10-year time frame.<sup>30</sup>

IRS closed 1,694 cases that TIGTA referred to the agency between fiscal years 2012 and 2021. Moreover, IRS closed the lowest number of UNAX cases during fiscal year 2020. Agency officials attributed the low closure rate for that year to a moratorium IRS imposed on effecting disciplinary actions beginning in March 2020 due to the COVID-19 pandemic. IRS officials told us this moratorium ended on May 31, 2020.

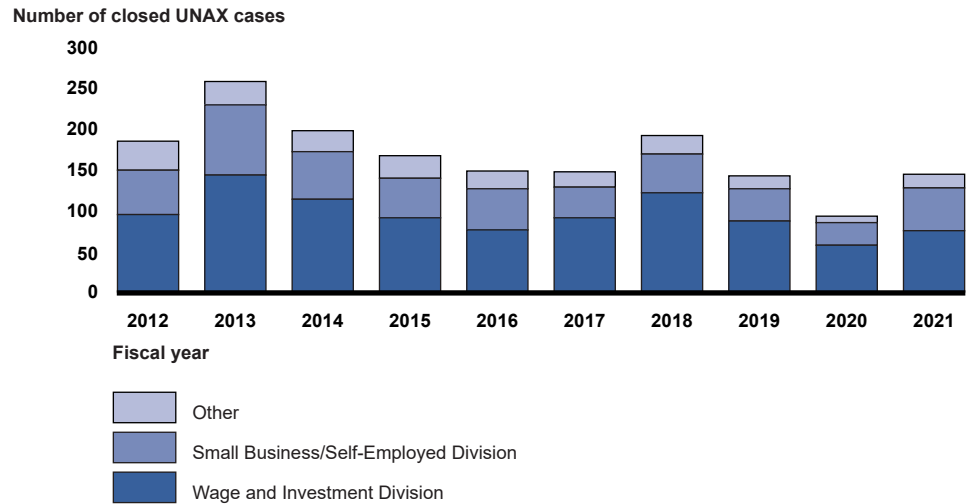
UNAX cases originated in 15 separate IRS business organizations over the last 10 years, but employees in the Wage & Investment Division (W&I) and Small Business/Self-Employed Division (SB/SE) account for more than 86 percent of all closed cases. As shown in figure 4, more than half of UNAX cases originated in W&I, and about 30 percent of cases originated in SB/SE.

<sup>28</sup>The Merit Systems Protection Board is an independent, quasi-judicial agency in the executive branch that serves as the guardian of federal merit systems.

<sup>29</sup>Employees can appeal final decisions that include removal; a suspension for more than 14 days; an indefinite suspension; a reduction in grade or a reduction in pay; and a furlough of 30 days or less of a full-time employee to the Merit Systems Protection Board in accordance with applicable law, or with the consent of the Union to binding arbitration. 5 U.S.C. § 7513(d); 5 C.F.R. § 752.405(a); Internal Revenue Service, *Internal Revenue Manual*, § 6.752.2.30 Rights to Appeal (Dec. 4, 2008).

<sup>30</sup>As stated above, these cases do not include IRS Chief Counsel employee cases, which comprise about 3 percent of IRS's workforce.

**FIGURE 4: CLOSED IRS EMPLOYEE UNAX CASES BY BUSINESS DIVISION, FISCAL YEARS 2012-2021**



Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data on closed cases of willful unauthorized access attempted access, or inspection of tax return or return information (UNAX). | GAO-22-105872

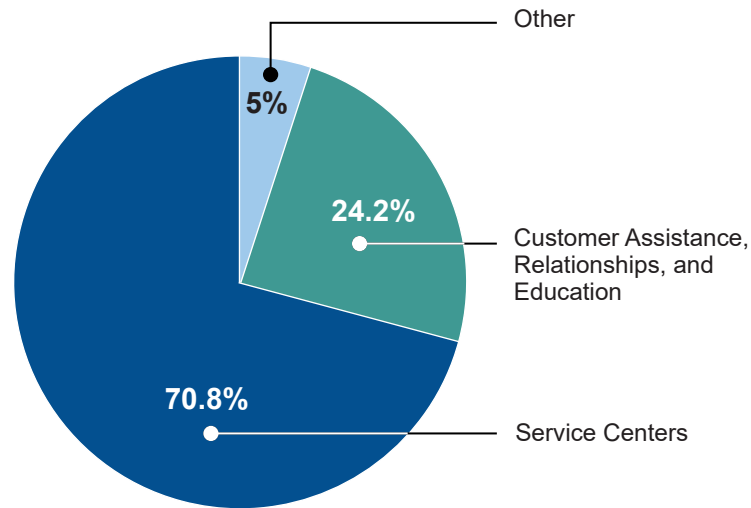
Notes: The cases in this figure are those that IRS opened beginning in fiscal year 2012 and closed by the end of fiscal year 2021. Other includes the following business units: Chief Financial Officer organization; Communications and Liaison; Criminal Investigations; Human Capital Office; Independent Office of Appeals; Information Technology; Large Business and International Division; National Headquarters; Taxpayer Advocate Service; Office of HR Operations; Office of Professional Responsibility; Privacy, Governmental Liaison and Disclosure; and Tax Exempt and Government Entities Division.

Between fiscal years 2015 and 2021, employees in W&I offices were involved in a greater percentage of UNAX investigations within IRS than their share of the agency population. During this time period, W&I's workforce accounted for about 42 percent of the overall IRS workforce, but accounted for approximately 58 percent of UNAX cases. According to knowledgeable IRS officials, W&I likely accounted for a greater percentage of UNAX cases than its share of the employee population because a greater percentage of W&I employees have access to federal tax information for their normal duties as compared to other business units.

IRS could not easily provide documentation of the percentage of employees in each business unit with regular access to federal tax information; however, IRS officials provided some context as to why a greater number of UNAX cases originated in W&I and SB/SE. According to IRS officials, as of April 21, 2022, more than 90 percent of the users for IRS's key system used to process tax information were employees in W&I or SB/SE. IRS officials also said that W&I compliance functions, in combination with SB/SE, process nearly all of transactions affecting taxpayer accounts after their return is filed, such as a tax refund payment or notice of balance due.

Within W&I, a majority of UNAX cases originated in Service Center Campuses.<sup>31</sup> According to IRS’s internal documentation, W&I Service Center employees accounted for approximately 35 percent of the IRS workforce while, based on our analysis, these employees were the subject of 40 percent of UNAX investigations during the same time period.<sup>32</sup> Within W&I, 70.8 percent of closed UNAX cases occurred in a Service Center and 24.2 percent occurred in the Customer Assistance, Relationships, and Education office (see fig. 5).<sup>33</sup>

**FIGURE 5: CLOSED IRS EMPLOYEE UNAX CASES BY WAGE AND INVESTMENT DIVISION, FISCAL YEARS 2012-2021**



Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data closed cases of willful unauthorized access, attempted access, or inspection of tax returns or return information (UNAX). | GAO-22-105872

Note: The cases in this figure are those that IRS opened beginning in fiscal year 2012 and closed by the end of fiscal year 2021.

Many W&I employees work in job functions that necessitate access to federal tax information, especially staff in the Service Centers and Customer Assistance, Relationships, and Education offices. W&I Service Centers house different functions, including answering tax law and tax account inquiries and adjusting tax accounts. According to IRS officials, W&I Service Center employees process all tax returns filed each year. In addition, they provide taxpayers with information on the status of their returns and refunds.

The Customer Assistance, Relationships, and Education office educates and communicates with taxpayers and provides face-to-face and virtual assistance to taxpayers, among other responsibilities. This office oversees Taxpayer Assistance Centers that provide face-to-face assistance to taxpayers related to many issues, including assisting

<sup>31</sup>These cases were from 10 different locations—Andover, Atlanta, Austin, Brookhaven, Cincinnati, Fresno, Kansas City, Memphis, Ogden, and Philadelphia—and included employees in Accounts Management, Compliance, Field/Identity Theft, and Submission Processing.

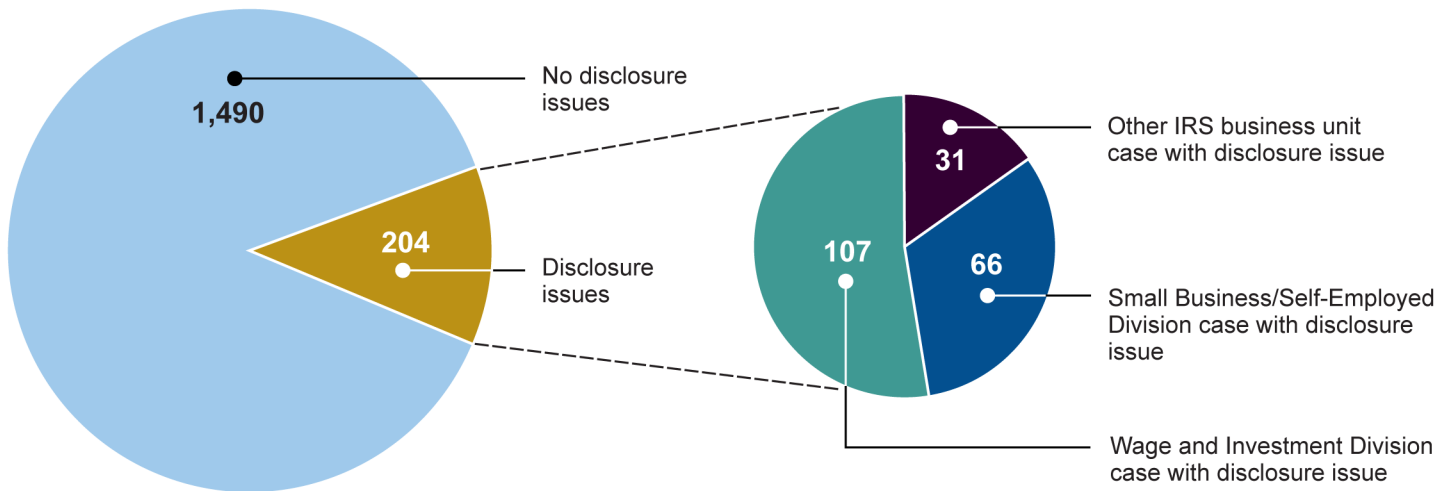
<sup>32</sup>IRS documentation did not include this calculation for fiscal years 2012, 2013, or 2014.

<sup>33</sup>Nationwide, W&I has approximately 37,000 employees located in 376 Taxpayer Assistance Centers, 10 Service Center Campuses, and 15 Remote Call Sites.

victims of identity theft refund fraud and providing transcripts of tax returns.

The number of unauthorized disclosure cases was lower than UNAX cases. Similar to UNAX cases, the majority of unauthorized disclosure cases were in W&I and SB/SE.<sup>34</sup> Of the 1,694 UNAX cases that IRS investigated and closed between fiscal years 2012 and 2021, 12 percent (204) included an investigated unauthorized disclosure issue (see fig. 6).

**FIGURE 6: NUMBER OF UNAX CASES WITH AN UNAUTHORIZED DISCLOSURE ISSUE, FISCAL YEARS 2012-2021**



Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data on closed cases of willful unauthorized access, attempted access, or inspection of tax return or return information (UNAX). | GAO-22-105872

Notes: The cases in this figure are those that IRS opened beginning in fiscal year 2012 and closed by the end of fiscal year 2021. Cases with a disclosure issue depicted in the graphic also contained a UNAX issue.

**HOW MANY UNAUTHORIZED ACCESS AND UNAUTHORIZED DISCLOSURE CASES DID IRS SUBSTANTIATE?**

IRS’s Human Capital Office, in conjunction with the employee’s supervisory chain, investigates cases and closes the case by making one of the following determinations:

- **Substantiated.** IRS determines that the facts support that the employee being investigated committed a violation of UNAX or unauthorized disclosure policy.<sup>35</sup>
- **Unsubstantiated.** IRS determines that there is not proof that a violation occurred. According to IRS officials, sometimes in investigations, the agency does not find evidence to substantiate a UNAX or unauthorized disclosure violation, but finds that the employee being investigated had other misconduct issues.<sup>36</sup>

<sup>34</sup>Overall, there were 1,229 cases that had a disclosure issue in the data. We could only confirm 204 of these were related to the unauthorized disclosure of federal tax information.

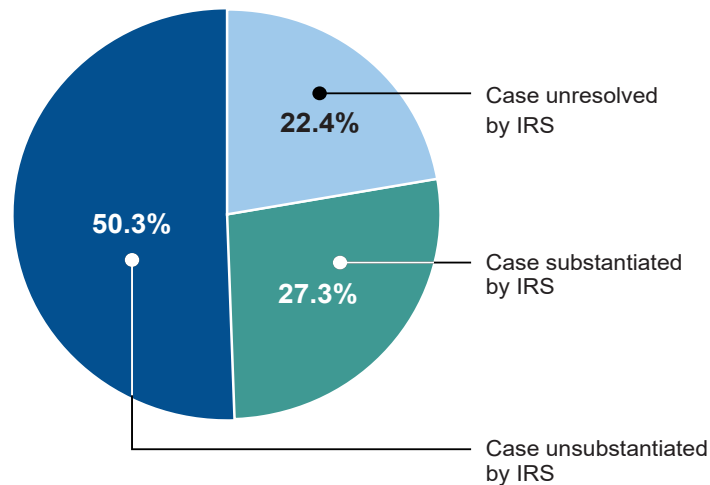
<sup>35</sup>If IRS adjudicates a case and issues a proposal letter to an employee and the employee resigns prior to IRS management rendering a decision, IRS considers the incident to be substantiated.

<sup>36</sup>Our analysis is based on IRS employee UNAX cases. We did not analyze characteristics of cases where IRS investigated employees for lesser unauthorized access or disclosure issues, such as inadvertent or negligent unauthorized access or disclosure.

• **Unresolved.** According to IRS officials, IRS closes cases as unresolved when the employee resigns, retires, or otherwise separates from the agency prior to adjudicating the case. This allows IRS to reopen the matter and adjudicate it if the employee is subsequently rehired.

As shown in figure 7, IRS substantiated 27 percent of closed UNAX cases as violations. Of the 1,694 UNAX cases IRS closed from fiscal years 2012 to 2021, the agency determined 462 cases to be violations. IRS closed 852 cases as unsubstantiated and 380 cases as unresolved.

**FIGURE 7: IRS SUBSTANTIATION OF CLOSED UNAX CASES, FISCAL YEARS 2012-2021**

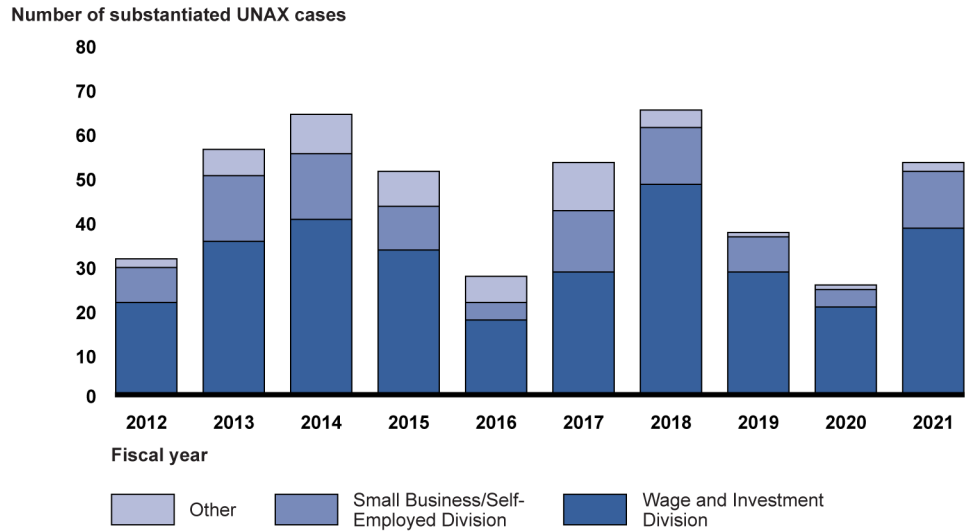


Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data on closed cases of willful unauthorized access, attempted access, or inspection of tax return or return information (UNAX). | GAO-22-105872

Note: The cases in this figure are those that IRS opened beginning in fiscal year 2012 and closed by the end of fiscal year 2021.

The distribution of substantiated UNAX cases among IRS offices generally matched the distribution of all closed UNAX cases over the 10-year time period. UNAX violations occurred in cases that originated within 10 different offices. As shown in figure 8, W&I and SB/SE employees committed the majority of UNAX violations.

**FIGURE 8: SUBSTANTIATED IRS EMPLOYEE UNAX CASES BY BUSINESS DIVISION, FISCAL YEARS 2012-2021**

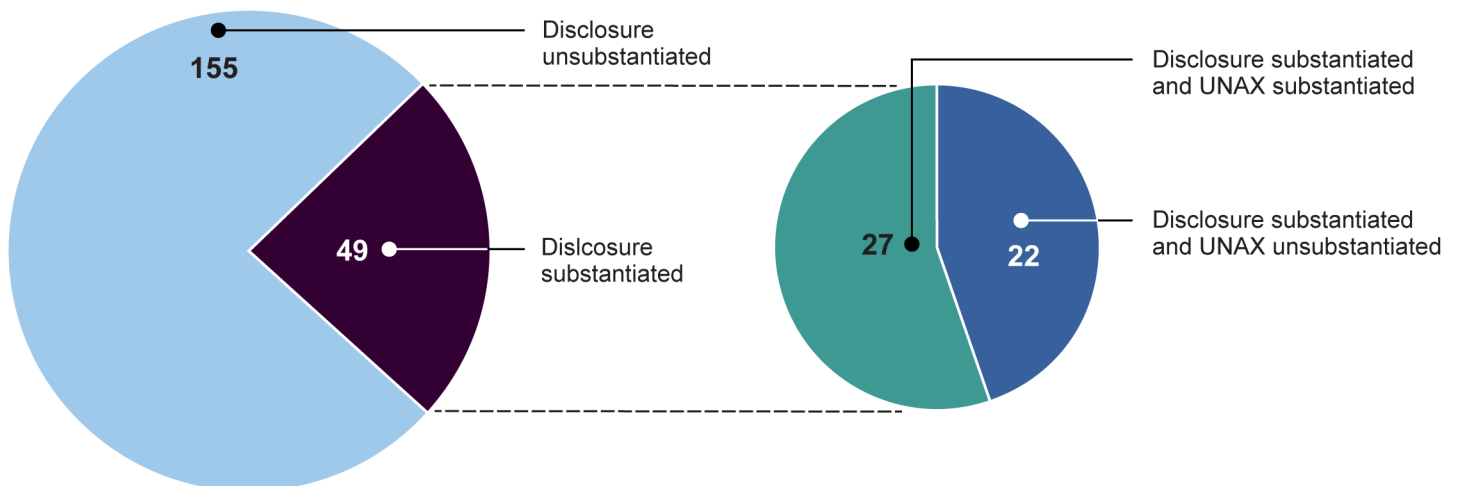


Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data on substantiated cases of willful unauthorized access, attempted access, or inspection of tax return or return information (UNAX). | GAO-22-105872

Notes: The cases in this figure are those that IRS opened beginning fiscal year 2012 and closed by the end of fiscal year 2021. Other includes the following business units: Criminal Investigations; Independent Office of Appeals; Information Technology Office; Large Business and International Division; National Headquarters; Taxpayer Advocate Service; Privacy, Governmental Liaison and Disclosure; and Tax Exempt and Government Entities Division.

Of the 204 UNAX cases that included an unauthorized disclosure issue, IRS substantiated 49 disclosure violations. In 27 of these cases, IRS found that the offending employee committed both a UNAX and an unauthorized disclosure violation (see fig. 9).

**FIGURE 9: IRS SUBSTANTIATION OF UNAUTHORIZED DISCLOSURE CASES, FISCAL YEARS 2012-2021**



Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data on closed cases of willful unauthorized access, attempted access, or inspection of tax return or return information (UNAX). | GAO-22-105872

Notes: Cases with a disclosure issue depicted in the graphic also contained a UNAX issue. The cases in this figure are those that IRS opened beginning in fiscal year 2012 and closed by the end of fiscal year 2021.

Cases that IRS does not substantiate may involve other issues of employee misconduct that were under investigation. Cases with a UNAX issue ranged from having no other assigned misconduct issues to eight additional issues under investigation. Issues that commonly co-occurred with UNAX issues were related to situations where employees made false statements or became involved in matters that resulted in a real or perceived conflict of interest with official duties.

## HOW LONG DO UNAUTHORIZED ACCESS INVESTIGATIONS TAKE?

Over the past 10 fiscal years, it has taken TIGTA and IRS, on average, a combined 464 days to investigate UNAX cases. On average, TIGTA took about 254 days to conduct its independent investigations. After receiving TIGTA's report, IRS officials generally took 211 days to close a case.<sup>37</sup>

Further, appealed cases can have especially long investigation times, although IRS's data on appeals may be incomplete.<sup>38</sup> Based on our analysis, IRS employees appealed at least 74 UNAX case penalty determinations between fiscal years 2012 and 2021. For the cases we could identify as having an employee appeal, IRS took an average of 409 days to close these cases in comparison to an average of 200 days for cases that were not appealed.

Since 2017, IRS has not met its timeliness goal for investigating and closing UNAX cases. According to the *Internal Revenue Manual*, IRS's goal for investigating and closing these cases is 180 days.<sup>39</sup> However, starting in 2017, IRS has taken 332 days on average to complete UNAX case investigations.

IRS officials cited staffing issues as the main cause of the longer investigation times in recent years. According to IRS officials, between fiscal years 2014 and 2015, the agency shut down a specialized unit that worked on UNAX investigations, a decision which officials said might have led to longer investigation times. After IRS disbanded this specialized team, IRS assigned UNAX investigation processing to the Human Capital Office's Labor/Employee Relations, Field Operations office that did not have a team with specialized UNAX processing expertise. Additionally, IRS officials said that by 2017, most of the remaining employees specializing in processing UNAX cases had retired. As IRS assembles additional teams, officials hope it will take less time for Human Capital Office specialists to process and close UNAX

<sup>37</sup>IRS Human Capital specialists working cases place them in a suspended status when circumstances beyond their control prevent timely case processing (e.g., government shutdowns or requesting additional information from TIGTA). According to IRS officials, IRS does not count the days a case is in suspended status in its calculation of case investigation time. However, for our calculations, we did not subtract the time cases were in suspended status in calculating case investigation time because we could not access the variable with suspension dates as it could contain federal tax information.

<sup>38</sup>When an employee appeals a disciplinary action, IRS Human Capital officials open a new case. These appeal cases are supposed to be linked to their original misconduct cases. In practice however, IRS officials stated that Human Capital officials may not systematically link cases.

<sup>39</sup>See Internal Revenue Service, *Internal Revenue Manual* § 6.751.1.1.18(1), Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance (Nov. 4, 2008).

cases. According to IRS officials, the Field Operations office is currently training experienced Labor Relations specialists to process UNAX cases, so that more staff can be assigned to work these cases.

## WHO COMMITS UNAUTHORIZED ACCESS AND DISCLOSURE VIOLATIONS?

The majority of UNAX and unauthorized disclosure violations during fiscal years 2012-2021 were committed by nonmanagerial employees. Managers accounted for less than 10 percent of UNAX and less than 15 percent of unauthorized disclosure violations. According to IRS data, during the same time period employees in the two most common managerial pay plans represented about 9 percent of the IRS employee population.

During this same period, permanent full-time employees committed most UNAX and unauthorized disclosure violations. About 74 percent of UNAX violations and 80 percent of unauthorized disclosure violations involved a permanent full-time employee. Full-time seasonal employees generally committed the remaining UNAX and disclosure violations.

There were no clear trends in UNAX violations committed by employee groups with similar tenure times at IRS. However, based on our analysis, IRS employees with less than 6 years of service and those with 21 or more years of service consistently had fewer substantiated cases relative to their proportion of IRS's workforce. Specifically, between fiscal years 2015 and 2021, employees with less than 6 years of service represented an average of 22 percent of IRS's overall workforce, but committed about 16 percent of UNAX violations for this time period.<sup>40</sup> IRS employees with 21 or more years of service represented between 27 and 36 percent of IRS's workforce, but committed about 23 percent of UNAX violations for this time period. All other employee groups committed a percentage of UNAX violations that were greater than their share of the workforce.

Similar to UNAX violations, there were no clear trends in disclosure violations by employee groups with similar years of service at IRS. Between fiscal years 2015 and 2021, employees with less than 6 years of tenure at the agency committed about 10 percent of disclosure violations while making up an average of 22 percent of the IRS workforce. IRS employees with 21 or more years of service represented between 27 and 36 percent of IRS's workforce, and committed about 35 percent of disclosure violations for this time period.

## WHAT HAPPENS TO UNAUTHORIZED ACCESS AND DISCLOSURE VIOLATORS IN SUBSTANTIATED CASES?

More than 82 percent of UNAX violations resulted in the offending employee's suspension, resignation, or removal (see table 1). Similarly, for the cases where IRS found employees committed both UNAX and unauthorized disclosure violations, all cases resulted in the offending employee's suspension, resignation, or removal.

<sup>40</sup>IRS calculated tenure group workforce percentage based on employee Service Computation Date, which is generally based on how long the person has been in the federal service. Because we did not have this variable for our analysis, we calculated the percentage of substantiated cases by tenure group based on employee Entered on Duty Date, which is the day the employee started at IRS, modified for any previous IRS service. For some employees these dates might be different which could cause some discrepancies in the comparison of workforce percentages to substantiated case percentages.



**TABLE 1: FINAL ACTIONS FOR UNAX CASES WHERE IRS SUBSTANTIATED THE ALLEGATIONS, FISCAL YEARS 2012-2021**

Final Action	Instances	Percentage
Suspensions	243	52.6
Resignation	35	7.6
Removal <sup>a</sup>	105	22.7
Other <sup>b</sup>	79	17.1
Total	462	100

Source: Internal Revenue Service (IRS) Automated Labor and Employee Relations Tracking System data on substantiated cases of willful unauthorized access, attempted access, or inspection of tax return or return information (UNAX). | GAO-22-105872

Notes: Percentages may not total 100 due to rounding. The cases in this table are those that IRS opened beginning in fiscal year 2012 and closed by the end of fiscal year 2021.

<sup>a</sup>Removals included in this count are for employees whose probation periods were complete.

<sup>b</sup>Other includes the following actions: alternative discipline in lieu of reprimand, alternative discipline in lieu of suspension, admonishment, caution letter, closed without adjudication, Closed Without Action cautionary letter, Closed Without Action letter, last chance agreement, probation/separation, reprimand, separation of temporary employee, and written counseling.

While IRS guidelines suggest specific penalties for certain offenses, managers have discretion in assigning penalties after considering many factors about the violation. Generally, the *Manager’s Guide to Penalty Determinations* suggests that the proposed final action for substantiated UNAX cases should be removal.<sup>41</sup> When an IRS employee attempts to access one’s own return information or that of a person in a covered relationship (such as a spouse or dependent child), the suggested penalty ranges from a 14-day suspension to removal.

When determining the final action, managers are to consider the nature and seriousness of the offense, potential for rehabilitation, mitigating circumstances, and consistency with other penalties, among other factors. While business units decide the supervisory authority needed to determine disciplinary actions, knowledgeable IRS officials said that the final penalty determination for UNAX cases is generally made by a manager two or three levels above the employee being investigated. Managers also take into account other substantiated issues under investigation associated with a UNAX case when assigning penalties.

<sup>41</sup>In our analysis we found that some UNAX violations did not have removal for their proposed final action. According to IRS officials, there are varying reasons for this, such as the employee resigned prior to the issuance of the proposed final action or the case had been misclassified as a UNAX case.

According to IRS documentation, in fiscal year 2021, the agency notified 51 taxpayers that their tax information was improperly accessed.<sup>42</sup> These notifications were the result of 11 UNAX violations.

According to TIGTA officials, between fiscal years 2012 and 2021, the Department of Justice accepted 35 employee UNAX or unauthorized disclosure cases for prosecution, of which 24 resulted in guilty outcomes. Between fiscal years 2012 and 2021, IRS closed 25 cases that had a criminal indictment returned against the employee being investigated.

---

<sup>42</sup>IRS is required to notify taxpayers whose information was accessed if the agency proposed disciplinary or adverse action against an employee for UNAX or unauthorized disclosure. 26 U.S.C. § 7431(e).

## AGENCY COMMENTS

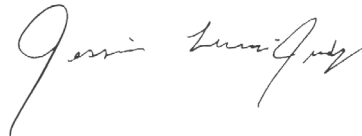
We provided a draft of this report to IRS and TIGTA for review and comment. In its comments, reproduced in appendix I, IRS said it takes its responsibility to prevent UNAX and unauthorized disclosures seriously as do the vast majority of IRS employees. IRS employees who commit these violations face serious discipline up to and including removal from IRS. IRS and TIGTA also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Commissioner of Internal Revenue, the Inspector General for Tax Administration and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact us at (404) 679-1831 or [FranksJ@gao.gov](mailto:FranksJ@gao.gov) and (202) 512-6806 or [LucasJudyJ@gao.gov](mailto:LucasJudyJ@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.



Jennifer R. Franks  
Director, Center for Enhanced Cybersecurity  
Information Technology and Cybersecurity



Jessica Lucas-Judy  
Director, Tax Issues  
Strategic Issues

## APPENDIX I: AGENCY COMMENTS

INTERNAL REVENUE  
SERVICE

DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, DC 20224

Ms. Jennifer R. Franks  
Ms. Jessica Lucas-Judy  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, DC 20548

Dear Ms. Franks and Ms. Lucas-Judy:

We reviewed the draft report entitled "Security of Taxpayer Information: Characteristics of IRS Employee Unauthorized Access and Disclosure Cases (GAO 105395)" and would like to provide a response and technical comments. The IRS takes a proactive approach to protecting the taxpayer information entrusted to us. Both the Privacy, Governmental Liaison and Disclosure (PGLD) and Cybersecurity operations educate IRS employees about their responsibilities to protect sensitive information. These education efforts encompass mandatory training and frequent communications about actions employees should take to protect information and IRS systems.

Similarly, the IRS takes its responsibility to prevent Unauthorized Access (UNAX) and unauthorized disclosures very seriously. As you describe in your report, the IRS has created a robust monitoring and reporting structure designed to identify UNAX and unauthorized disclosures, investigate cases and adjudicate any findings of inappropriate conduct by employees and contractors. IRS employees are constantly reminded that they are only to access taxpayer information that is directly related to their casework. Any instances of UNAX or intentional unauthorized disclosure are unacceptable and are treated with the upmost seriousness as reflected in the disciplinary actions faced by employees and contractors who do not follow the law.

The vast majority of IRS employees take their charge to protect taxpayer information as the foundation of their career in serving America's taxpayers. The small number of employees who do not uphold our standards face serious discipline up to and including removal from the IRS. We will continue to educate our employees and refine our capabilities to detect UNAX and unauthorized disclosures as these efforts are key to ensuring that taxpayers can trust that the information provided to the IRS will be protected and only used for legitimate tax administration purposes.

We have attached a listing of technical comments for your review and consideration. If you have any questions, please contact me, or a member of your staff may contact Robert Choi, IRS Chief Privacy Officer, at 202-317-6449.

Sincerely,

Jeffrey J. Tribiano  
Deputy Commissioner for  
Operations Support

Enclosure

## APPENDIX II: AGENCY CONTACTS

**GAO Contacts**

Jennifer R. Franks at (404) 679-1831 or [FranksJ@gao.gov](mailto:FranksJ@gao.gov).

Jessica Lucas-Judy at (202) 512-6806 or [LucasJudyJ@gao.gov](mailto:LucasJudyJ@gao.gov).

**Staff Acknowledgments**

In addition to the contacts named above, Mark Canter (Assistant Director), Jason Vassilicos (Assistant Director), Dawn Bidne (Analyst-in-Charge), Kisa Bushyeager, Cassidy Cramton, Stephen Duraiswamy, Michele Fejfar, Robert Gebhart, Jackson Gode, Krista Loose, Ahsan Nasar, Robert Robinson, Daniel Swartz, Andrew J. Stephens, and Rachel Stoiko made key contributions to this report.



## GAO SUPPORT

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people.

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at <https://www.gao.gov>.

A. Nicole Clowers, Managing Director, Congressional Relations,  
clowersa@gao.gov, (202) 512-7114  
Chuck Young, Managing Director, Public Affairs,  
youngc1@gao.gov, (202) 512-4800

U.S. Government Accountability Office,  
441 G Street NW, Washington, DC 20548

Source: JSTOCK/stock.adobe.com (cover photo).

## CONGRESSIONAL REQUESTER

The Honorable Mike Crapo  
Ranking Member  
Committee on Finance  
United States Senate

