OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

KWAME RAOUL
ATTORNEY GENERAL

December 19, 2025

RE: Social Security Number Protection Task Force Report
to: **Task Force Member/Designated Recipient**

Dear Designated Task Force Recipient,

In accordance with 20 ILCS 4040/10, attached for your review and records is a copy of the Social Security Number Protection Task Force Report for 2025.

Thank you.

Best Regards,
Carolyn Friedman

Carolyn Friedman, CIPP/US
Task Force Chair
Supervisor, Privacy & Data Security Unit
Assistant Attorney General Illinois
Attorney General's Office

Enclosure: 2025 Task Force Report

Social Security Number Protection Task Force

Report to Governor J.B. Pritzker, Attorney General Kwame Raoul,
Secretary of State Alexi Giannoulias, and Illinois General Assembly
December 19, 2025

CONTENTS

TASK FORCE BACKGROUND

The Social Security Number (SSN) remains the key piece of sensitive personally identifiable information that identity thieves use to commit fraud. The SSN was intended to be used solely to distribute Social Security benefits, but in the years since its inception in 1935, it has been also used as a unique identification number. The SSN is therefore not only tied to an individual's credit report, financial records, and Social Security earnings with the federal government, but is also present in employment, educational, health, insurance, and criminal records. The wide dissemination of SSNs increases the likelihood that the numbers can be accessed and subsequently used for fraudulent purposes.

Consumers are therefore encouraged to limit their exposure to identity theft by protecting their SSNs. Businesses are also encouraged to do their part by taking necessary steps to limit the collection of SSNs, protect SSNs in their possession, and dispose of documents containing SSNs in a manner that renders them unusable. Local and state government agencies also have a role in protecting SSNs they maintain and reducing their continued widespread dissemination. Government agencies have the larger task of maintaining a system of open records for the public, while taking measures to reduce the amount of sensitive personally identifiable information in those records.

The General Assembly created the Social Security Number Protection Task Force (Task Force) through Public Act 93-0813 in 2004. The Task Force is charged with examining the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN when the State requires the individual to provide that number to an officer or agency of the State. The Task Force also is required to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs by State and local governments for identification and record-keeping purposes. In 2007, the General Assembly amended the law governing the Task Force by Public Act 95-0482. The Office of the Attorney General is charged with chairing and administering the activities of the Task Force.

Membership Of The Task Force –

- Two members representing the House of Representatives, appointed by the Speaker of the House – ***Awaiting Additional Member Appointment Confirmation*, Representative Ann Williams**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – ***Awaiting Additional Member Appointment Confirmation,* Representative Dan Ugaste**
- Two members representing the Senate, appointed by the President of the Senate – ***Awaiting Member Appointment Confirmation***
- Two members representing the Senate, appointed by the Minority Leader of the Senate - ***Awaiting Member Appointment Confirmation***
- One member representing the Office of the Attorney General – **Carolyn Friedman, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**
- One member representing the Office of the Governor – **Warren Wilke**

- One member representing the Department of Natural Resources – **John "J.J." Pohlman**
- One member representing the Department of Healthcare and Family Services – **Elizabeth Festa**
- One member representing the Department of Revenue – **Angela Hamilton**
- One member representing the Department of State Police – **Captain Felix Canizares**
- One member representing the Department of Employment Security – **Joseph Mueller**
- One member representing the Illinois Courts – **James Morphew**
- One member representing the Department on Aging – **Jessica Klaus**
- One member representing Central Management Services – **Jake Altman**
- One member appointed by the Executive Director of the Board of Higher Education – **Dr. Eric Lichtenberger**
- One member appointed by the Secretary of Human Services – **Sean Reddington**
- Three members representing local-governmental organizations – ***Awaiting Member Appointment***
- One member representing the Office of the State Comptroller – **Ben Haley**
- One member representing school administrators, appointed by the State Superintendent of Education – **Sara Boucek**

PART I: PROTECTION OF SSNS IN THE PUBLIC RECORD

The first statutory requirement of the Social Security Number Protection Task Force Act is to examine the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN.

IDENTITY PROTECTION ACT

One way to limit the unauthorized disclosure of SSNs is to limit their collection in the first place. If fewer entities collect and use SSNs, fewer entities are capable of disclosing those numbers improperly.

The Identity Protection Act, 5 ILCS 179/1 *et seq.*, prohibits certain collections, uses and disclosures of an individual's SSN by any person, or State or local government agencies. Specifically, the Act, with several exceptions, prohibits a person, or State or local government agency from collecting, using, or disclosing a SSN unless: (1) required to do so under state or federal law or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the agency's duties and responsibilities; (2) the need and purpose for the SSN is documented before the request; and (3) the SSN collected is relevant to the documented need and purpose. The need and purpose for the collection and use of SSNs must be documented in a written Identity-Protection Policy.

Each local government agency must file a written copy of its policy with the governing board of the unit of local government within 30 days after approval of the policy. Under Section 37(b), "each State agency must provide a copy of its identity-protection policy to the Social Security Number Protection Task Force within 30 days after the approval of the policy." State agencies

were reminded of this requirement on August 24, 2011. Policies can be submitted to the Task Force by mailing a copy to:

Illinois Attorney General
Social Security Number Protection Task Force
c/o: Carolyn Friedman
500 S. Second Street
Springfield, IL 62701

As part of the implementation of the policies, local and state agencies will require that all employees identified as having access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. Training should include instructions on the proper handling of information that contains SSNs from the time of the collection of the information through its destruction.

Identity-Protection Policies were to have been implemented within 12 months of the date of approval and a copy was to have been sent to the Task Force no later than June 1, 2012. For reference, an Identity-Protection Policy and Statement of Purpose(s) template can be found in Appendixes A and B.

Updated and/or amended Identity-Protection Policies may be sent electronically to SSNPolicy@ilag.gov. Submissions shall occur as soon as practicable or within the calendar year in which the updated amendment was implemented. An acknowledgement of receipt and record will be provided by a duly authorized representative of the Task Force chairperson.

(Template Identity-Protection Policy – Appendix A)
(Template Statement of Purpose(s) – Appendix B)

NEW DEVELOPMENTS IN LAWS AND REGULATIONS TO PROTECT SOCIAL SECURITY NUMBERS: Laws and regulations must be regularly updated to combat identity fraud and theft and safeguard personal information, while also ensuring access to personal information when necessary and appropriate.

On February 28, 2024, President Biden signed Executive Order 14117 titled Preventing Access to American's Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern. As part of the Executive Order's initiative to curb the distribution of bulk and sensitive data, including SSNs, the Department of Justice (DOJ) was tasked with drafting a final rule to restrict such transfers to foreign adversaries. The federal Cybersecurity and Infrastructure Security Agency (CISA) announced the finalized security recommendations for restricted transactions after a public notice and comment period to the DOJ on January 8, 2025. After reviewing the public feedback, CISA recommended that organizations could undertake restricted transactions so long as they had de-identified or pseudo anonymized the sensitive information, including SSNs.

(Federal Register: Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117– Appendix C)

Based on the CISA recommendations, on April 11, 2025, the Department of Justice National Security Division (NSD)'s Data Security Program (DSP) released a report outlining controls on the exporting of U.S. Government-related data and bulk U.S. sensitive data from being accessed by foreign adversaries. The DSP Compliance Guide outlines that U.S. individuals and entities need to know the volume and kind of data collected or maintained on U.S. persons, how the company uses the data, whether they engage in covered data transactions with covered persons or countries of concern, how the data is marketed and what information is included concerning current or former employees or contractors, and/or former U.S. government officials. The guidance went into effect in a staggered rollout, first requiring compliance with on April 8, 2025 with all sections except the due diligence and audit requirements. A NSD cure period for civil enforcement ran from April 8, 2025 to July 8, 2025, allowing U.S. Persons acting in good-faith the opportunity to come into compliance with the new guidelines. Full compliance came into effect on October 6, 2025, requiring a data compliance program to execute the audit and due diligence requirements for U.S. persons engaging in any restricted transaction involving sensitive data, including SSNs.

(NSD Data Security Program - Implementation and Enforcement Policy for First 90 Days - 04112025– Appendix D)

PART II: SSNS INTERNAL IDENTIFIERS

The second requirement of the Task Force is to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs for identification and record-keeping purposes by State and local governments. State and local government agencies continue to internally assess the collection and use of SSNs. Such an assessment was critical in drafting Identity-Protection Policies.

MINIMIZING THE USE OF SOCIAL SECURITY NUMBERS

Social security numbers have become both an identifier and an authenticator. Partly due to the proliferation of data breaches exposing consumer SSNs, minimizing use of SSNs has become increasingly important.

Part of the initiative to minimize the use of SSNs is to help educate consumers to have heightened awareness any time they are being requested to produce personal information, especially SSNs. The Illinois Attorney General's Office publishes Consumer Alerts throughout the year to raise awareness of specific scams or attempts to collect information for nefarious purposes.

As the income tax filing deadline approached, the Illinois Attorney General's Office published a consumer alert outlining guidance to help Illinois residents safely file tax returns and urged people to exercise caution before providing personally identifying and financial information online. Scammers will attempt to steal personal information to use it to file a tax return and potentially steal the tax returns from the consumer. As part of this consumer alert, consumers

were instructed to protect their SSN and to not give it out without being certain of the receiving party.

(*** CONSUMER ALERT*** ATTORNEY GENERAL RAOUL URGES RESIDENTS TO TAKE PRECAUTIONS TO AVOID TAX IDENTITY THEFT WHEN FILING TAX RETURNS – Appendix E)

On August 6, 2025, the Illinois Attorney General's Office published an alert warning about Back-to-School Scams, reminding consumers not to give out private information, including Social Security Numbers, in email, text messages, or chat bubbles. Scammers will often capitalize on current events, such as Back-to-School shoppers, to try to trick consumers into paying for services or items that they will likely never receive or share personal data that scammers can then use to steal consumers' identities.

(*** CONSUMER ALERT*** ATTORNEY GENERAL RAOUL WARNS ABOUT BACK-TO-SCHOOL SCAMS – Appendix F)

On November 26, 2025, the Illinois Attorney General's Office published a consumer alert urging consumers to shop with caution around the holidays. It outlines many potential risks to consumers personal information and SSNs including the importance of avoiding fake or fraudulent websites and reiterated the importance of not putting a SSN into anything unsecure such as an email, text message, or chat messaging where the data is not protected.

(*** CONSUMER ALERT*** ATTORNEY GENERAL RAOUL URGES CONSUMERS TO DO THEIR HOLIDAY SHOPPING WITH CAUTION – Appendix G)

The Illinois Attorney General's office will continue to educate consumers and publish alerts on how to minimize or limit sharing SSNs to third parties to reduce the risks of emerging scams as technology advances and the risks and dangers evolve.

CONCLUSION

Identity-Protection Policies at local and state government agencies throughout Illinois continue to be implemented according to the requirements of the Identity Protection Act. Over the course of the last year the Task Force has continued to monitor state-level discussions regarding further contemplated protections for Illinois individuals' Social Security numbers, and has also monitored federal bills involving the protections and restrictions associated with using Social Security numbers as individual identifiers. The Task Force will continue to monitor state and federal activities, recommending updates as needed and will continue to work together with all stakeholders to identify the best ways to protect SSNs in public records and limit the use of SSNs as internal identifiers.

APPENDIX A – Template Identity-Protection Policy

[AGENCY]
IDENTITY-PROTECTION POLICY

The [AGENCY] adopts this Identity-Protection Policy pursuant to the Identity Protection Act. 5 ILCS 179/1 *et seq*. The Identity Protection Act requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy to ensure the confidentiality and integrity of Social Security numbers agencies collect, maintain, and use. It is important to safeguard Social Security numbers (SSNs) against unauthorized access because SSNs can be used to facilitate identity theft. One way to better protect SSNs is to limit the widespread dissemination of those numbers. The Identity Protection Act was passed in part to require local and State government agencies to assess their personal information collection practices, and make necessary changes to those practices to ensure confidentiality.

Social Security Number Protections Pursuant to Law

Whenever an individual is asked to provide this Office with a SSN, [AGENCY] shall provide that individual with a statement of the purpose or purposes for which the [AGENCY] is collecting and using the Social Security number. The [AGENCY] shall also provide the statement of purpose upon request. That Statement of Purpose is attached to this Policy.

The [AGENCY] shall not:

1) Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.
2) Print an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity.
3) Require an individual to transmit a Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.
4) Print an individual's Social Security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the Social Security number to be on the document to be mailed. SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the Social Security number. A Social Security number that is permissibly mailed will not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

In addition, the [AGENCY] shall not[1]:

1) Collect, use, or disclose a Social Security number from an individual, unless:
    i. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the [AGENCY]'s duties and responsibilities;
    ii. the need and purpose for the Social Security number is documented before collection of the Social Security number; and
    iii. the Social Security number collected is relevant to the documented need and purpose.
2) Require an individual to use his or her Social Security number to access an Internet website.
3) Use the Social Security number for any purpose other than the purpose for which it was collected.

Requirement to Redact Social Security Numbers

The [AGENCY] shall comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's Social Security number. The [AGENCY] shall redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.

When collecting Social Security numbers, the [AGENCY] shall request each SSN in a manner that makes the SSN easily redacted if required to be released as part of a public records request. "Redact" means to alter or truncate data so that no more than five sequential digits of a Social Security number are accessible as part of personal information.

Employee Access to Social Security Numbers

---

[1] These prohibitions do not apply in the following circumstances:

(1) The disclosure of Social Security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's Social Security number will be achieved.

(2) The disclosure of Social Security numbers pursuant to a court order, warrant, or subpoena.

(3) The collection, use, or disclosure of Social Security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.

(4) The collection, use, or disclosure of Social Security numbers for internal verification or administrative purposes.

(5) The disclosure of Social Security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.

(6) The collection or use of Social Security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

Only employees who are required to use or handle information or documents that contain SSNs will have access. All employees who have access to SSNs are trained to protect the confidentiality of SSNs.

APPENDIX B – Template Statement of Purpose(s)

What does the [AGENCY] do with your Social Security Number?
Statement of Purpose for Collection of Social Security Numbers
Identity-Protection Policy

The Identity Protection Act, 5 ILCS 179/1 *et seq*., requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy that includes a statement of the purpose or purposes for which the agency is collecting and using an individual's Social Security number (SSN). This statement of purpose is being provided to you because you have been asked by the [AGENCY] to provide your SSN or because you requested a copy of this statement.

Why do we collect your Social Security number?

You are being asked for your SSN for one or more of the following reasons:
[THE FOLLOWING PURPOSES MAY NOT APPLY; IDENTIFY PURPOSES APPROPRIATE FOR YOUR AGENCY]

- Complaint mediation or investigation;
- Crime victim compensation;
- Vendor services, such as executing contracts and/or billing;
- Law enforcement investigation;
- Child support collection;
- Internal verification;
- Administrative services; and/or
- Other:_____

What do we do with your Social Security number?

- We will only use your SSN for the purpose for which it was collected.
- We will not:
    - Sell, lease, loan, trade, or rent your SSN to a third party for any purpose;
    - Publicly post or publicly display your SSN;
    - Print your SSN on any card required for you to access our services;
    - Require you to transmit your SSN over the Internet, unless the connection is secure or your SSN is encrypted; or
    - Print your SSN on any materials that are mailed to you, unless State or Federal law requires that number to be on documents mailed to you, or unless we are confirming the accuracy of your SSN.

Questions or Complaints about this Statement of Purpose

Write to the [AGENCY]:
[CONTACT INFORMATION]

APPENDIX C—Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117

AGENCY:

Cybersecurity and Infrastructure Security Agency (CISA), DHS.

ACTION:

Notice of availability

SUMMARY:

CISA is announcing publication of finalized security requirements for restricted transactions pursuant to Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." In October 2024, CISA published proposed security requirements for restricted transactions which would apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). CISA solicited comment on those proposed security requirements and considered that public feedback when developing the final security requirements. This notice also provides CISA's responses to the public comments received.

DATES:

January 8, 2025.

ADDRESSES:

Docket: For access to the docket to read background documents or comments received, go to *www.regulations.gov,* and insert the docket number, CISA-2024-0029, into the "Search" box, and follow the prompts.

FOR FURTHER INFORMATION CONTACT:

Alicia Smith, Senior Policy Counsel, Cybersecurity and Infrastructure Security Agency, *EOSecurityReqs@cisa.dhs.gov,* 202-316-1560.

SUPPLEMENTARY INFORMATION:

I. Background

On February 28, 2024, the President issued E.O. 14117 entitled "Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern" (the "Order"), pursuant to his authority under the Constitution and laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) ("IEEPA"), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of Title 3, United States Code. In the Order, the President expanded the scope of the national emergency declared in E.O. 13873 of May 15, 2019, "Securing the Information and Communications Technology and Services Supply Chain," and further addressed the national emergency with additional measures in E.O. 14034 of June 9, 2021, "Protecting Americans' Sensitive Data from

Foreign Adversaries." Specifically, Section 2(a) of E.O. 14117 directs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, to issue, subject to public notice and comment, regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction: (i) involves bulk sensitive personal data or United States Government-related data, as defined by final rules implementing the Order; (ii) is a member of a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in the Order; and (iii) meets other criteria specified by the Order.[1]

Among other things, the Order, at Section 2(c), instructs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, to issue regulations identifying specific categories of transactions ("restricted transactions") that meet the criteria described in (ii) above for which the Attorney General determines that security requirements, to be established by the Secretary of Homeland Security through the Director of CISA, adequately mitigate the risks of access by countries of concern or covered persons [2] to bulk sensitive personal data or United States Government-related data. In turn, Section 2(d) directs the Secretary of Homeland Security, acting through the Director of CISA, to propose, seek public comment on, and publish those security requirements. Section 2(e) delegates to the Secretary of Homeland Security the President's powers under IEEPA as necessary to carry out Section 2(d).

On October 29, 2024, CISA published a Federal Register notice, Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117 (the "October 29 Request for Comment"), announcing the release of the "Proposed Security Requirements for Restricted Transactions" [3] directed by E.O. 14117 Section 2(d) and requesting public comment on the proposal. *See*89 FR 85976. The proposed security requirements were developed to apply to the classes of restricted transactions identified in DOJ's notice of proposed rulemaking (NPRM), "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," and published in the Federal Register on the same day as the proposed security requirements. *See*89 FR 86116.

The DOJ NPRM proposed to require, consistent with E.O. 14117, that United States persons engaging in restricted transactions must comply with the final security requirements by incorporating the standards by reference. *See* proposed 28 CFR 202.248, 202.401, 202.402.

The security requirements were divided into two sections: organizational- and covered system-level requirements (Section I) and data-level requirements (Section II). The listed requirements were selected with the intent of directly mitigating the risk of access to covered data, with additional requirements included to ensure effective governance of that access, as well as approaches for establishing an auditable basis for compliance purposes. The security requirements further included a definitions section. To the extent the requirements used a term

already proposed to be defined in the DOJ rulemaking, CISA's use of that term in the security requirements would carry the same meaning. The October 29 Request for Comment described the proposed security requirements and definitions, and further provided a non-exhaustive list of twelve questions to assist members of the public in formulating their comments.

CISA received 24 comments on the proposed security requirements and considered them while developing the final security requirements. Comments submitted in response to the October 29 Request for Comment are available in the docket associated with this notice available at *https://www.regulations.gov* (Docket CISA-2024-0029). DOJ's NPRM received 75 comments, which are available in the docket associated with that NPRM at *https://www.regulations.gov* (Docket DOJ-NSD-2024-0004-0001). DOJ shared comments with CISA that DOJ received in response to the NPRM that provided feedback that could impact the security requirements. These comments include one confidential comment that contained CISA equities and was provided to DOJ by a foreign government.

II. Response to Public Comments

A. In General

CISA reviewed and considered all comments received in response to the October 29 Request for Comment. Overall, many commenters appreciated the flexibility that CISA provided regarding implementation of the security requirements as well as the use of existing frameworks. Some commenters, however, felt that application of the security requirements as proposed may be burdensome. Others requested clarification of certain definitional terms and the scope of the security requirements. Some commenters also provided specific feedback on technical elements of the proposed security requirements. CISA addresses those comments in the following sections and explains where CISA made changes to its proposal to address the feedback received.[4]

B. Specific Topics

1. Responses to Questions in CISA's Notice

In the October 29 Request for Comment, CISA included a non-exhaustive list of twelve questions to assist the public in providing comments in response to the notice. *See*89 FR 85980. The comments CISA received on those questions, and CISA's adjudication of those comments, are summarized below.

Robustness, Burden, and Flexibility of Proposed Security Requirements

In the October 29 Request for Comment, CISA solicited comments on whether the proposed security requirements were sufficiently robust to mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern (question 1). CISA also asked whether the security requirements provided sufficient flexibility for the types of restricted transactions typically engaged in by U.S. entities to avoid overburdening commercial activities not involving covered data (question 3).[5]

Many commenters either suggested or explicitly stated that the security requirements were sufficiently robust to mitigate the risk of access to covered data by countries of concern, but may

be too prescriptive or burdensome to implement.[6] For instance, while commenters generally appreciated CISA's use of established frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a small number of commenters questioned whether CISA's security requirements extend beyond those frameworks and suggest more prescriptive mandates that may be difficult to implement.[7] Other commenters acknowledged that organizations that will be required to comply with this rule already employ some level of sophisticated cyber defense measures, but it will take time for organizations to understand, interpret, and fully implement the requirements,[8] particularly for small- and medium-sized businesses.[9] One financial sector association noted that, for financial institutions with large, diverse networks, implementation would be resource-intensive and may not be feasible in some circumstances.[10]

Several commenters expressed appreciation for the flexibility embedded in the data-level requirements in Section II, noting that flexibility encourages a risk-based but tailored approach to securing transactions, and would help ensure the requirements stay up-to-date as standards are updated and technology advances.[11] For that reason, many commenters encouraged CISA to extend such flexibility to the organizational- and system-level requirements in Section I.[12]

Some commenters suggested that organizations be permitted to employ alternative compensating controls on covered systems where requirements are otherwise infeasible.[13] Others urged CISA to model the security requirements on existing regulatory regimes administered by other U.S. government agencies (*e.g.,* the Federal Communications Commission and the Department of Commerce), which direct organizations to develop cyber risk management plans aligned with the CSF, or create avenues for reciprocity in instances where U.S. entities entering into restricted transactions are subject to and have demonstrated compliance with certain existing data or cybersecurity regulatory regimes.[14] Commenters suggested that not providing the requested flexibility, modeling, or reciprocity would increase the burden on parties engaged in restricted transactions.[15]

CISA considered these options but ultimately concluded that the overall structure and approach of the original security requirements provide as much flexibility as reasonably practicable while still addressing the national security risks identified by DOJ. CISA assesses that granting reciprocity where U.S. entities entering into restricted transactions are subject to and have demonstrated compliance with certain existing data or cybersecurity regulatory regimes is not a workable solution to address the national security risks associated with restricted transactions. Other regulatory regimes are not necessarily designed to address the specific risks at issue here. Therefore, CISA cannot assume that a cyber risk management plan developed to comply with another regulatory regime will necessarily be designed in a way that mitigates the risk of covered persons or countries of concern gaining access to covered data. Further, even if CISA were to do a comparison to map the security requirements against the requirements in other regulatory regimes and identify existing regulatory regimes that cover all of the security requirements today, CISA could not control for the possibility that those regulations may be changed to no longer align with the security requirements, particularly in light of the different goals of these regulations.

That said, CISA is taking a number of steps to make the final security requirements less burdensome and address specific concerns about technical feasibility or ease of implementation with respect to individual requirements. Specifically in the following sections of the security requirements:

- I.A.1.a: CISA acknowledges the challenge of maintaining an accurate asset inventory in dynamic environments, and revises I.A.1.a to require documented inventories only "to the maximum extent practicable," and eliminated the requirement to inventory MAC addresses, which is not possible in some situations such as cloud environments. CISA also clarified that these inventories can themselves be dynamically curated.
- I.A.3: CISA addresses commenters' concerns about the rigidity, utility, and feasibility of the proposed vulnerability remediation timelines, and substantially revises the vulnerability remediation timelines to prioritize critical assets and allow entities engaged in restricted transactions to remediate vulnerabilities within a risk-informed span of time. CISA assesses that these new requirements appropriately balance the risks of exploitation of vulnerable covered systems with the operational burden of patching systems.
- I.A.5: In response to comments about the level of effort required to implement the security requirements across large enterprises,[16] CISA revises the requirement for any network interfacing with a covered system to facilitate visibility into connections between assets to be implemented "to the extent technically feasible" instead of "to the maximum extent practicable."
- I.A.6: To grant organizations additional flexibility in how they choose to perform change management, CISA significantly reduces the burden around installation of new hardware and/or software by removing the reference to "firmware" and requirements for either allowlists or approvals to address specific software versions.[17]
- I.B.2: CISA seeks to introduce flexibility and alleviate confusion around the meaning of the term "immediately" by revising the requirement to revoke access to covered systems for terminated employees or employees with changed roles from "immediately" to "promptly," with clarifying examples of what would be considered "promptly." CISA recognizes the ambiguity of "immediately" and assesses that the clarifying examples appropriately balance operational complexity and the security benefits of promptly revoking access to covered data upon termination or change of an employee's role.
- I.B.3: Acknowledging the term "disabled" is ambiguous and that commenters requested CISA clarify that the requirement was to implement a process, CISA clarifies language around security log retention to state that organizations are required to implement a notification process when security logs are not being produced and/or retained as expected rather than referring to logs being disabled.
- I.B.4 [removed]: To reduce burden on implementing organizations, CISA removes the requirement to maintain organizational policies and processes to ensure that unauthorized media and hardware are not connected to covered assets. CISA assesses that in light of

CISA's updates to the definition of the term "covered system," the other requirements are sufficient to protect covered systems, and this requirement is no longer necessary. [Note that, as a result of this deletion, requirements I.B.5 and 6 are now I.B.4 and 5.]

- I.B.5 [renumbered I.B.4] CISA clarifies that deploying "deny by default" is not as burdensome as some commenters assumed by noting the idea of "deny by default" does not only include the use of network firewalls but may also be implemented in other ways, such as via authentication of users and other information systems to the covered system. CISA assesses that, as clarified, this requirement is important to ensure that unauthorized systems and users do not inappropriately have access to data within covered systems.

At the same time, when crafting the proposed security requirements, CISA did so with the goal of balancing regulatory burden, technical feasibility, and flexibility with the underlying national security needs. As such, CISA determined that certain recommendations, such as extending the flexible implementation approach in the data-level requirements to the organizational- and system-level requirements, would undermine security to the detriment of the overall regime. CISA notes that the organizational- and system-level requirements are scoped only to a limited subset of covered systems that interact with data of particular sensitivity (per the DOJ rule) and are neither considered nor intended to comprise the entirety of an effective cybersecurity program; rather, they are a selected set of practices and preconditions that CISA concluded are necessary to effectively implement the data-level requirements.

Clarifying Terms and Applications

CISA asked whether the security requirements were sufficiently clear for organizations to verify compliance (question 3) and/or sufficient to provide U.S. persons engaged in restricted transactions confidence that the logical and physical access controls are sufficiently managed to deny access to covered persons or countries of concern (question 2). CISA also asked about areas where additional interpretive guidance would be helpful to U.S. entities in determining which data-level requirements should be applied based on the nature of the transaction and the data at hand (question 6).

Some commenters requested that CISA clarify the definition of "covered system," specifically as it relates to endpoints (*e.g.,* workstations/laptops), to make clear that the definition only applies to systems that handle covered data qualified as bulk under DOJ's definition.[18] One commenter observed that "this interpretation is of critical importance as it represents the difference between organizations considering how they secure a collection of specific systems as opposed to an enterprise-wide retooling, the latter of which would be extremely challenging and unnecessarily burdensome." [19]

In response, CISA revises the definition of "covered system" to reflect that a covered system is limited to systems that interact with covered data in bulk form and not user endpoints that ordinarily read or view sensitive personal data (other than sensitive personal data that constitutes government-related data) but do not ordinarily interact with sensitive personal data in bulk form. Of note, because government-related data is not subject to any bulk data threshold in the DOJ rulemaking, any system that interacts with government-related data would still be considered a

covered system. Organizations implementing the security requirements need to carefully consider how this clarification applies to their particular information systems, transactions, and manners of interacting with covered data.

CISA also received comments requesting that, in defining "covered systems" and "covered data," CISA include an explicit reference to exempt transactions by specifically exempting data that is subject to an exemption from the definition of covered systems and covered data.[20]

CISA notes that both definitions in the security requirements require the system and/or data to be used "as part of a restricted transaction." Per the definitions in the DOJ rulemaking, an exempt transaction is definitionally not a restricted transaction and thus an information system that *exclusively* participates in transactions with covered persons that are exempt (*e.g.,* an internal human resources system that only deals in data subject to the corporate group exemption) would not be considered a covered system under the definition. Because CISA assesses that the definition already excludes such systems, CISA does not make any changes to the definition in response to these comments. However, consistent with changes to the DOJ rulemaking to switch the order of the terms "government-related data" and "bulk U.S. sensitive personal data" to avoid the possibility of confusion as to whether the bulk thresholds apply to government-related data, CISA has revised the definition of "covered data" to switch the order of these terms in the definition.

Mapping to Other Frameworks

In the October 29 Request for Comment, CISA inquired about the utility of mapping requirements to other standards, such as ISO/IEC 27001 or NIST Special Publication 800-171 (question 12). Some commenters recommended this approach, noting that such mapping would be helpful to allow organizations to better understand how existing processes or controls they are already using can be applied and understood in the context of the security requirements.[21] Other commenters suggested additional candidates (*e.g.,* CISA's Encrypted DNS Implementation Guidance).[22]

CISA determined additional mapping is better suited to interpretive guidance because these frameworks include detailed security control sets, and such guidance will need to further clarify the intent and extent of the mapping to these controls. CISA decided not to include additional mapping in the final security requirements themselves but remains open to providing additional mapping through future interpretive guidance.

2. Other Comments on the Security Requirements

Extent to Which Covered Persons May Access Covered Data

Several commenters inquired if CISA's security requirements were intended to prevent all access to covered data by covered persons or to prevent unauthorized or unmitigated access.[23] That is, commenters sought clarity on whether any degree of access by covered persons to covered data is permissible when implementing the security requirements. Commenters noted, for instance, that the chapeau of Section II of the security requirements indicated that entities were required to prevent covered persons or countries of concern from gaining access to covered data, which

would appear to render the transaction no longer covered by DOJ's rule.[24] Commenters explained that under their reading, the requirement to prevent access to covered data by covered persons or countries of concern arguably takes the transaction out of the DOJ rule's definition of restricted transaction altogether.[25] Commenters noted, however, that CISA's security requirements were developed to suggest the efficacy of controls such as data minimization, masking, and privacy-enhancing techniques in mitigating the risk of access to covered data by covered persons or countries of concerns.

To address the feedback raised in these comments, CISA affirms that the security requirements are meant to prevent access to covered data by countries of concern unless specific efforts outlined in the security requirements are taken to mitigate the national security risks associated with such access.

More specifically, in the chapeau to the data-level requirements in Section II, CISA proposed that U.S. persons should "implement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data by covered persons and/or countries of concern." CISA proposed that this approach would mitigate the national security risks associated with access to covered data by covered persons and/or countries of concern. As described in the Order, DOJ's NPRM, and CISA's proposed security requirements and the October 29 Request for Comment, access to covered data by covered persons and/or countries of concern poses a range of threats to national security and foreign policy, including providing countries of concern with information they need or can use to engage in malicious cyber-enabled activities and malign foreign influence; blackmail and espionage against U.S. persons; intimidate activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. *See*89 FR 85978. In the security requirements, CISA proposed to address these risks at the data level by requiring that covered persons be denied access to the underlying covered data—either by denying access outright or by only allowing covered persons access to covered data that had been manipulated in a way (*e.g.,* encryption, de-identification) that would effectively mitigate the risks from permitting direct access to the underlying data.

In response to comments on this issue, CISA clarifies the chapeau language for the data-level requirements in the final security requirements to state that U.S. persons should "implement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered *data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology* by covered persons and/or countries of concern." This clarification establishes that the adoption of the data-level requirements does not mean no access to covered data is permissible, but that certain data-level requirements must be implemented to achieve a level of minimization of that access and/or covered data sufficient to mitigate the national security risks identified by DOJ.

Under the DOJ regulation, covered data transactions include regulated categories of transactions that involve covered person or country of concern access to covered data, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified. As DOJ explains in its

rulemaking, encryption, pseudonymization, and de-identification are not completely effective in all cases and can in some cases be reversed or undermined. At the same time, the transactions identified by DOJ as restricted have important economic value relative to their national security risk and are allowed to proceed if they meet the CISA-developed security requirements. CISA was thus tasked with determining an appropriate balance on mitigating the national security risks associated with such access to covered data.

While CISA considered whether it could adopt other options for data-level requirements that would still permit access to at least some unmitigated covered data to covered persons, CISA ultimately determined that allowing covered persons or countries of concern access to covered data without application of an effective combination of techniques identified in the data-level requirements (such as pseudonymization, de-identification, aggregation, and encryption) would not effectively mitigate the unacceptable national security risks identified by DOJ resulting from enabling access to such data by covered persons and countries of concern. Thus, the final security requirements permit organizations to undertake restricted transactions either by directly denying covered person/country of concern access to covered data itself or by applying techniques such as pseudonymization, de-identification, aggregation, and encryption in the manner prescribed in the security requirements to reduce the risks to national security while still allowing for a form of access to an appropriately mitigated version of the covered data (in conjunction with implementation of the organizational- and system-level requirements).

As noted in the DOJ regulation's definition of access, the implementation of data processing techniques (as outlined in the data-level requirements) before sharing data is irrelevant to the determination of whether a transaction involves “access” and is thus a covered data transaction. However, restricted transactions are explicitly permitted to proceed through application of the security requirements, effectively mitigating the national security risks identified by DOJ.

The following examples discuss several applicable scenarios. In all cases (with the exception of example 4), these examples assume that the organization has conducted the required data risk assessment required in Section I.C of the security requirements and determined that the specific requirements implemented are sufficient to “fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern.” The examples (with the exception of example 4) also assume that the organization complies with other applicable requirements in the DOJ's rule.

Example 1: A U.S. person retains a cloud provider headquartered in a country of concern to store encrypted covered data through a vendor agreement. Per the DOJ rulemaking, the cloud provider is a covered person, and such a transaction would constitute a covered data transaction. The U.S. person implements the security requirements, including the requirements around encryption and encryption keys. Such a transaction could proceed if the U.S. person fully implements the security requirements.

Example 2: A U.S. business that deals in covered data is executing an investment agreement with a covered person. The investment agreement provides that the U.S. business will share with the

covered person investor sensitive personal data about individual consumers that meets DOJ's relevant bulk threshold. The organization implements the security requirements before sharing data with the covered person investor (for example by aggregating data and/or de-identifying it along with implementing the other security requirements). Such data is still considered covered data. The sharing of data in the investment agreement is still a restricted transaction but can proceed due to the implementation of the security requirements.

Example 3: A U.S. organization hires a covered person in a country of concern (or retains their services by contract) into a role whose duties include access to covered data. As part of entering into the employment agreement (or vendor agreement), the organization implements the security requirements (including the organizational- and system-level requirements) and only shares de-identified covered data with the covered person in a way that minimizes linkability in accordance with the security requirements. Such a restricted transaction would be allowed to proceed.

Example 4: Same as Example 3, except that instead of de-identifying the covered data, the organization knowingly authorizes the employee or vendor to have access to covered data (*e.g.,* to bulk U.S. sensitive personal data) without applying efforts to de-identify, pseudonymize, encrypt, or otherwise implement the data-level security requirements. In this example, the U.S. organization knowingly gave a covered person access to covered data through an employment or vendor agreement without implementing the security requirements. As such, the U.S. organization knowingly engaged in a restricted transaction that fails to comply with the requirements of subpart D of 28 CFR part 202 and thus is engaged in a covered data transaction that is not authorized pursuant to 28 CFR 202.401.

Example 5: Same as Example 3, except the employee or vendor's duties do not require access to covered data but do include general access to the organization's networks and information systems, including potentially covered systems, within which covered data may be stored. The organization implements the security requirements, including the data-level requirement of denying access to covered data for that covered person. Because the transaction could afford a covered person access to covered data, but the organization employed controls to prevent it, such an employment or vendor agreement could proceed as a restricted transaction.

Vulnerability Management (I.A.3)

In the proposed security requirements, CISA proposed that organizations should patch vulnerabilities that are known to be exploited, critical, or high within an outlined timeframe. CISA proposed this approach for consistency with the standard to which Federal Agencies are held under Binding Operational Directives (BOD) 22-01 and 19-02. CISA received several comments on this subject suggesting that CISA's approach was technically challenging to implement and not sufficiently risk-based.[26] One commenter, for instance, stated that the remediation timelines proposed were too aggressive, and noted that NIST Special Publication 800-53 directs remediation to occur in accordance with a risk-assessment rather than prescribing specific timelines.[27] Another commenter recommended that CISA change the timelines for remediation to no shorter than 30 days, stating that CISA's proposed timeframes of 14 and 15 days were unreasonable and impracticable.[28] Commenters indicated that this requirement may

cause organizations to expend their limited resources addressing vulnerabilities that do not necessarily pose the greatest risk to their organizations.[29]

CISA considered this feedback carefully and concluded that an alternate approach to vulnerability management could effectively respond to the identified risks while being less burdensome in implementation. In the final security requirements, CISA adopts a new approach that requires organizations to remediate known exploited vulnerabilities (KEVs) in internet-facing systems in a risk-based manner that prioritizes the most critical assets first, with all such vulnerabilities remediated within 45 calendar days. This approach is based on the approach to patching outlined in the CISA Cross-Sector Cybersecurity Performance Goals (CPGs) and the CSF. To compensate for the additional flexibility being provided through the revised requirement, CISA determined that it was necessary to require that entities engaged in restricted transactions establish a process to evaluate, after patching, whether any internet-facing covered systems with KEVs were compromised prior to the patch being applied. Based on its operational experience, CISA notes that KEVs on internet-facing systems are commonly exploited with access persisting beyond the time of patching. A KEV is a vulnerability that is currently being exploited, based on information known to CISA.[30] Through this change, CISA intends to reduce the operational burden of vulnerability management and maximize its impact on addressing known cybersecurity risks to covered systems.

Multi-Factor Authentication and Password Length (I.B.1)

In the proposed security requirements, CISA proposed that organizations should implement multi-factor authentication (MFA) for access to covered systems or, if not technically feasible and/or enforced, implement passwords of a minimum of 16 characters. CISA proposed this approach based on the CSF and the CISA CPGs. Commenters suggested that CISA's approach would be clearer if CISA incorporated NIST Special Publication 800-63B (SP 800-63B)'s definition of Authentication Assurance Levels (AALs) and only required 16-character passwords if technically feasible.[31]

In the final security requirements, CISA added a reference to NIST's AAL definition to clarify that CISA considers any authenticator that implements AAL2 or AAL3 (as defined in the latest version of SP 800-63B or any of its supplements) as qualifying as MFA for purposes of this requirement. This includes syncable cryptographic authenticators (colloquially known as “passkeys”). However, CISA notes that “Multi-factor authentication” is a broadly understood term in the industry and declines to remove its use from the security requirements. CISA also updates the requirement for 16-character passwords to instead require 15-character passwords in situations without MFA. This change reduces burden on organizations and aligns CISA's requirement with the CPGs. However, CISA declines to further reduce the number of required characters, even where 15-character passwords are not technically feasible. This requirement is taken from the CISA CPGs where sufficiently strong passwords are suggested for all password-protected IT assets, with an understanding that some operational technology (OT) assets may not be able to technically support such passwords. CISA does not believe such OT assets are likely to host covered data and did not receive any comments suggesting otherwise. CISA concludes that information systems that host covered data be required to either implement MFA (including

“passwordless” methods) or have 15-character minimum passwords in instances where MFA is not technically feasible and/or enforced (such as when MFA is partially enforced due to technical limitations). CISA believes that organizations should implement MFA in all situations where it is technically feasible to do so and where it is not, must ensure 15-character passwords are used in covered systems. CISA assesses that this approach is a reasonable requirement that is well grounded in industry best practices. Technologies such as password managers may be used to reduce the operational burden of such passwords.

Access To Log Systems (I.B.3)

One commenter [32] requested that CISA clarify whether authorized access to the security logging system is intended to be limited to those users who are authorized to access the covered system itself or, more generally, users performing security duties in the organization.

CISA declines to make any changes to the text of the final security requirements in response to this comment, but notes that the security requirements specify that users who access or modify such log data are only required to be “authorized and authenticated.” CISA does not intend that individuals who are “authorized and authenticated” to access or modify collected logs must also be authorized to access covered systems.

Data Risk Assessment (I.C)

Several commenters raised questions and concerns about the data risk assessment. Some commentors were concerned about whether the risk assessment was to be shared with DOJ or CISA, while others had some concerns about the potential cost impact and compliance burden of developing it. Others also noted that DOJ included audit and reporting requirements in its rule and that the addition of another compliance report under CISA's requirements would be too burdensome.[33]

In response to these comments, and to deconflict with DOJ's audit and reporting requirements, CISA makes minor changes to this requirement, specifically clarifying this risk assessment is intended for internal use only as a tool to inform data protection (not for documentation or disclosure to a government agency), and, to further reduce implementation burden, that documenting the assessment is not required.[34] CISA also supplies additional detail specifying that the plan be reviewed internally by the organization.

Data-Level Requirements and What Constitutes “Sufficiency” (II, Chapeau)

Comments pertaining to the data-level requirements were largely positive, noting an appreciation for the level of flexibility that was perceived by many to be in contrast with the system-level requirements. For instance, one commenter said that allowing organizations flexibility to determine which combination of data-level requirements are sufficient to address risks, based on their unique risk profile “presents the best chance of achieving Executive Order 14117's ultimate objective to secure” sensitive U.S. data.[35] However, some commenters took issue with the requirement to *fully* and effectively prevent access to covered data, and requested guidance and/or clarification about what constitutes a “sufficient” combination of data-level requirements

to prevent access. CISA also received some feedback from interagency partners on further clarifying the specific encryption requirements.

Given that commenters generally agreed that the data-level requirements as written achieved their intended aim, CISA made only minor revisions. Commenters asked CISA to clarify that requirements around the version of Transport Layer Security (TLS) used were limited to connections that were already using TLS, which CISA clarified by including requirements for the version of TLS in II.B.1 rather than as a separate requirement (II.B.2). CISA also consulted with other federal agency partners on the topic of encryption and is adding an explanation of what level of encryption CISA considers sufficient for the purposes of these security requirements based on these consultations. CISA recognizes the appeal of a prescriptive (and predictable) standard but maintains there is no one-size-fits-all solution given the varied nature of restricted transactions. Additionally, the question of what is sufficient to prevent access is a compliance matter and not a technical implementation matter. E.O. 14117 sec. 2(d)(ii) gives the Attorney General authority to issue enforcement guidance regarding these security requirements, in consultation with the Director of CISA. CISA will coordinate with DOJ if it determines further guidance on the meaning of "sufficient" is appropriate.

Framework Mapping

Many commenters expressed appreciation for the fact that CISA leveraged existing, well-known cybersecurity and privacy frameworks, and found the mapping between frameworks and specific requirements especially helpful. However, some commenters expressed concern that CISA's approach was not conducive to harmonizing cyber regulations to the greatest degree practicable across the government and suggested that CISA's mapping to the CSF, NIST's Privacy Framework (PF), and CPGs may be confusing, noting that the CSF is the primary risk management framework used by some organizations.

After considering these comments, CISA continues to assess that its method of mapping the security requirements to the CSF, PF, and CPGs is the optimal way to minimize the burden on organizations while still allowing as much flexibility in implementation as possible.

First, as noted in the proposed security requirements and as CISA has preserved in the final security requirements, references to these frameworks are intended to help readers understand which aspects of existing frameworks, guidance, or other resources the security requirements are based upon; understanding and applying the security requirements *does not* require a reader to understand and apply those references. As such, the references should only serve to be a helpful reference where readers find them useful, while those who find the references confusing or who do not use these other resources as part of their organizational compliance structure can disregard the mapping.

Second, the Order requires CISA to base its security requirements on the CSF and the PF. CISA has evidenced compliance with this requirement by reference to these frameworks explicitly. This means that the only framework CISA could eliminate the mapping to is the CPGs. Given that many commenters expressed appreciation for the CPG mapping and that the CPGs are, themselves, based on the CSF, CISA assesses that the inclusion of the CPGs should not be overly

difficult or confusing, especially for the cybersecurity personnel and designated accountable officials responsible for ensuring that U.S. entities engaging in restricted transactions adhere to the final security requirements.

3. Out of Scope or Related to DOJ's NPRM

Several commenters raised questions, concerns, or feedback that were outside of the authorities and direction provided to CISA in E.O. 14117. Commenters also raised issues that were related to the implementation of DOJ's regulations rather than the proposed security requirements themselves.

While CISA reviewed this feedback and shared relevant comments with DOJ to consider as they drafted their final rule, issues specific to the DOJ rule itself are beyond the scope of this notice. Conversely, in some instances, DOJ received comments on its NPRM that more directly related to CISA's proposed security requirements. Where DOJ shared such comments with CISA, CISA reviewed and considered this feedback as part of developing the final security requirements, as reflected above.

4. Continued Stakeholder Engagement

CISA also received a few comments requesting additional stakeholder engagement on the development of these security requirements. For example, one comment requested an extension of the comment period by 17 days to provide stakeholders extra time to provide robust and considered input.

CISA appreciates the commenters' desire to provide the most useful, robust, and thoughtful feedback possible in the time allotted for comments. However, CISA decided not to extend the comment period given the pressing national security interests underlying the need for DOJ's rule, and E.O. 14117's requirement that the rule incorporate CISA's security requirements.

Other commenters requested that CISA establish an ongoing stakeholder engagement process to receive continued feedback on the security requirements even after they have been finalized. Some of the commenters noted that these security requirements could be burdensome to implement effectively, and others emphasized that experience applying the security requirements could lead stakeholders to identify areas for improvement.

CISA appreciates stakeholder interest in ensuring that the security requirements remain current and applicable over time and will consider the best way to receive and incorporate relevant feedback in the future to the extent changes to the security requirements become necessary or desirable. However, at this time, CISA does not intend to establish a formal process for receiving additional feedback on the security requirements given that the comment period has closed, and CISA must finalize the security requirements so that they can be incorporated by reference into DOJ's final rule.

One commenter expressed concern about the security requirements being a “quasi-rule,” indicating that CISA could change the security requirements at any point in the future without “procedural protections” for impacted entities.[36]

CISA appreciates the concern raised by the commenter and confirms that CISA has no intention of changing these security requirements without providing the public notice of any future changes. As discussed above, CISA notes that while the Order directed DOJ to propose a rule and finalize that rule to implement its directive, the Order did not provide the same direction to CISA for promulgating the security requirements. By design, the security requirements themselves are not a rule governed by the process laid out in the Administrative Procedure Act, 5 U.S.C. 553. While this allows CISA to update the security requirements quickly, tracking new developments in technology and data security, such updated security requirements will not be enforceable against entities regulated by DOJ's rule unless DOJ updates its rule to change the version of the security requirements incorporated therein by reference. In other words, commenters can be assured that they will not be subjected to new security requirements without receiving requisite procedural protections for implementing the change, as required by law.

III. Description of Final Security Requirements

The security requirements are intended to address national-security and foreign-policy threats that arise when countries of concern [37] and covered persons access U.S. government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. Additional background on the purpose for these security requirements was included in CISA's notice announcing the release of the proposed security requirements. *See*89 FR 85978. The DOJ Final Rule requires, consistent with E.O. 14117, that United States persons engaging in restricted transactions comply with the final security requirements by incorporating the security requirements by reference into the regulations. 28 CFR 202.401.

The security requirements remain divided into two sections: organizational- and covered system-level requirements (Section I) and data-level requirements (Section II). The listed requirements were selected with the intent of directly mitigating the risk of access to covered data, with additional requirements included to ensure effective governance of that access, as well as approaches for establishing an auditable basis for compliance purposes. Requirements that directly mitigate the risk of access include I.B.1-2, I.B.4-5, and all data-level requirements (II.A, II.B, II.C, and II.D). Requirements included as a mechanism for ensuring proper implementation and governance of those access controls include all controls in I.A. Additional requirements incorporated as a mechanism for ensuring auditable compliance of the aforementioned access controls include I.B.3 and I.C. These requirements reflect a minimum set of practices that CISA assesses are required for effective data protection, as informed by CISA's operational experience. These requirements were designed to be representative of broadly accepted industry best practices and are intended to address the needs of national security without imposing an unachievable burden on industry.

The final security requirements largely maintain the same design as the proposed security requirements. The security requirements are designed to mitigate the risk of sharing U.S. government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions.[38] They do this by imposing conditions specifically on the *covered data* that may be accessed as part of a restricted transaction, on the *covered systems* more broadly (both terms CISA defines within the security requirements), and

on the organization as a whole. While the requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA continues to assess that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of which persons may have access to different data sets.

In addition to requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to unmitigated covered data. The security requirements provide multiple options to mitigate risk, though all the options build upon the foundation of the requirements imposed on covered systems and the organization as a whole. While U.S. persons [39] engaging in restricted transactions will be required to implement all the organizational- and system-level requirements, such persons will have some flexibility to determine which combination of data-level requirements are sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, based on the nature of the transaction and the data at issue.

Finally, the security requirements include a definitions section. To the extent the requirements use a term already defined in the DOJ rulemaking, CISA's use of that term in the security requirements would carry the same meaning. For the purpose of these security requirements, CISA includes definitions for five terms used exclusively in the security requirements:

- *Asset.* CISA defines the term to mean data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. This definition is derived from the CSF version 1.1, which defined asset as "[t]he data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes."
- *Covered data.* CISA defines the term to mean the two categories of data identified by the Order and that DOJ is regulating through its rulemaking—government-related data or bulk U.S. sensitive personal data.
- *Covered system.* CISA defines this term as a specific type of information system that is used to conduct a number of activities related to covered data as part of a restricted transaction. These activities are drawn from a combination of the activities in the

definition of information system in the security requirements and the activities in the DOJ rulemaking's definition of access. See 28 CFR 202.201. The term means an information system used to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, view, receive, collect, process, maintain, use, share, disseminate, or dispose of (collectively, "interact with") covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified. "Covered system" does not include an information system (*e.g.,* an end user workstation) that has the ability to view or read sensitive personal data (other than sensitive personal data that constitutes government-related data) but does not ordinarily interact with such data in bulk form.

- *Information system.* CISA defines this term consistent with the definition in the Paperwork Reduction Act (PRA), 44 U.S.C. 3502.[40] The term means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- *Network.* CISA defines this term, which CISA developed consistent with the definition of the term in NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* The term would mean a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

The publication of the finalized security requirements for restricted transactions pursuant to Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" can be found on CISA's website: *https://www.cisa.gov/resources-tools/resources/EO-14117-security-requirements*. The Director of CISA, Jennie M. Easterly, has delegated the authority to approve and electronically sign this document to Nitin Natarajan, who is the Deputy Director of CISA, for purposes of publication in the Federal Register .

Nitin Natarajan,

Deputy Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

Footnotes

1. The other criteria do not directly impact the development of the security requirements but are related to DOJ's implementation of the Order's directive via their regulations. See E.O. 14117, sec. 2(a)(iii)—(v), 89 FR 15421, 15423 (Mar. 1, 2024).

Back to Citation

2. Section 2(c)(iii) of the Order requires the Attorney General to identify, with the concurrence of the Secretaries of State and Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of the Order.

Back to Citation

3. The proposed security requirements were posted at *https://www.cisa.gov/resources-tools/resources/proposed-security-requirements-restricted-transactions*.

Back to Citation

4. CISA also participated in several stakeholder engagement sessions organized by DOJ. While CISA did not receive written feedback during these sessions, many points raised by stakeholders in these sessions were echoed in the written comments received in response to the October 29 Request for Comment.

Back to Citation

5. Other aspects of question 3 related to the clarity and specificity of the security requirements are addressed separately below.

Back to Citation

6. *See, e.g.,* Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by ACT|The App Association, CISA-2024-0029-0001.

Back to Citation

7. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

Back to Citation

8. *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.

Back to Citation

9. *See, e.g.,* Comment submitted by Consumer Technology Association, CISA-2024-0029-0013.

Back to Citation

10. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

Back to Citation

11. *See, e.g.,* Comment submitted by Workday, CISA-2024-0029-0019.

Back to Citation

12. *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017; Comment submitted by Workday, CISA-2024-0029-0019; Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by ACT|The App Association, CISA-2024-0029-0001.

Back to Citation

13. *See, e.g.,* Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015.

Back to Citation

14. *See, e.g.,* Comment submitted by CTIA—The Wireless Association and NCTA—The internet & Television Association, CISA-2024-0029-0021; Comment submitted by USTelecom—The Broadband Association, CISA-2024-0029-0018.

Back to Citation

15. *See, e.g.,* Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017; Comment submitted by Workday, CISA-2024-0029-0019; Comment submitted by Oracle, CISA-2024-0029-0014.

Back to Citation

16. *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA 2024-0029-0017.

Back to Citation

17. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

Back to Citation

18. *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.

Back to Citation

19. Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.

Back to Citation

20. *See, e.g.,* Comment submitted by WorkDay, CISA-2024-0029-0019.

Back to Citation

21. *See, e.g.,* Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by ACT|The App Association, CISA-2024-0029-0023.

Back to Citation

22. *See, e.g.,* Comment submitted by Infoblox, CISA-2024-0029-0020.

Back to Citation

23. *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017; Comment submitted by the Consumer Technology Association, CISA-2024-0029-0013; Comment submitted by National Foreign Trade Council, CISA-2024-0029-0022.

Back to Citation

24. *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.

Back to Citation

25. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

Back to Citation

26. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011; Comment submitted by Consumer Technology Association, CISA-2024-0029-0013; Comment submitted by USTelecom, CISA-2024-0029-0018; Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015.

Back to Citation

27. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011

Back to Citation

28. *See, e.g.,* Comment submitted by Consumer Technology Association, CISA-2024-0029-0013.

Back to Citation

29. *See, e.g.,* Comment submitted by the Bank Policy Institute, CISA-2024-0029-0011.

Back to Citation

30. *See generally* Cybersecurity and Infrastructure Security Agency, Reducing the Significant Risk of Known Exploited Vulnerabilities, *https://www.cisa.gov/known-exploited-vulnerabilities* (last visited Dec. 1, 2024) (listing CISA's requirements for listing a KEV).

Back to Citation

31. *See, e.g.,* Comment submitted by Workday, CISA-2024-0029-0019; Comment submitted by USTelecom—The Broadband Association, CISA-2024-0029-0018.

Back to Citation

32. See Comment submitted by The Business Software Alliance, CISA-2024-0029-0024.

Back to Citation

33. *See, e.g.,* Comment submitted by The Consumer Technology Association, CISA-2024-0029-0013.

Back to Citation

34. CISA defers to DOJ regarding whether such a risk assessment may be subject to audit or other review as part of compliance aspects of the DOJ rulemaking.

Back to Citation

35. *See, e.g.,* Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

Back to Citation

36. *See, e.g.,* Comment submitted by The Business Software Alliance, CISA-2024-0029-0024.

Back to Citation

37. Terms used in CISA's security requirements that are defined in the DOJ rulemaking have the same meaning in the security requirements as provided in the DOJ rulemaking.

Back to Citation

38. CISA notes that the security requirements are, as required by the Order, designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's CPGs, available at *https://www.cisa.gov/cross-sector-cybersecurity-performance-goals,* are not reflected in the proposed data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber incidents.

Back to Citation

39. As noted above, for the purposes of the security requirements, to the extent CISA uses a term that is defined in the DOJ rulemaking, CISA uses that definition. Therefore, CISA is using the term U.S. persons as defined by the DOJ Final Rule. That definition reads "any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States." 28 CFR 202.256.

Back to Citation

40. 6 U.S.C. 650(14) (which applies to all of Title XXII of the Homeland Security Act of 2002, which, in turn, contains most of CISA's authorities) defines Information System as having the meaning given the term in the Paperwork Reduction Act, 44 U.S.C. 3502, and specifically includes "industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers." 6 U.S.C. 650(14). However, given CISA's assumption that this type of operational technology is unlikely to be implicated by DOJ's regulations, CISA is not including the operational technology-related prong here.

Back to Citation

[FR Doc. 2024-31479 Filed 1-3-25; 8:45 am]

BILLING CODE 9111-LF-P

Federal Register :: Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117

APPENDIX D—Department of Justice National Security Division Foreign Investment Review Section, DATA SECURITY PROGRAM: IMPLEMENTATION AND ENFORCEMENT POLICY THROUGH JULY 8, 2025

April 11, 2025

The Data Security Program ("DSP") implemented by the National Security Division ("NSD") under Executive Order 141171 comprehensively and proactively addresses the continued efforts of foreign adversaries to use commercial activities to access, exploit, and weaponize U.S. Government-related data and Americans' bulk sensitive personal data. The DSP addresses this "unusual and extraordinary threat… to the national security and foreign policy of the United States" that has been repeatedly recognized across political parties and by all three branches of Government—including, notably, in the 2025 Annual Threat Assessment of the U.S. Intelligence Community and the President's America First Investment Policy, NSPM-2 on Imposing Maximum Pressure on Iran, national emergency declared in Executive Order 13873, 2 and 2017 National Security Strategy. To address this urgent threat, the DSP establishes what are effectively export controls that prevent foreign adversaries, and those subject to their control and direction, from accessing U.S. Government-related data and bulk U.S. sensitive personal data. NSD's primary mission with respect to the implementation and enforcement of the DSP is to protect U.S. national security from the risk caused by countries of concern that seek to collect and weaponize Americans' most sensitive personal data. The International Emergency Economic Powers Act ("IEEPA") and the DSP authorize NSD to bring civil enforcement actions and criminal prosecutions for knowing or, with respect to criminal prosecutions, willful violations of the DSP's requirements. Unlawful acts under IEEPA are subject to civil penalties of up to the greater of $368,136 or twice the value of each violative transaction. Willful violations of IEEPA are punishable by imprisonment of up to 20 years and a $1,000,000 fine. As the final rule explained, this threat is increasingly urgent, and ensuring prompt compliance with the DSP's requirements is critical to addressing the Administration's priorities and stopping the flow of U.S. sensitive personal data and government-related data to countries of concern. As explained in more detail in the DSP Compliance Guide, to aid compliance with the DSP requirements, U.S. individuals and entities should "know their data," including the kind and volume of data collected or maintained concerning U.S. persons; how their company uses this 1 Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern). On January 8, 2025, NSD issued a final rule implementing Executive Order 14117, which is now available at 28 CFR Part 202. Unless otherwise indicated, all citations are to the sections of the DSP regulations in 28 CFR part 202. 2 Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). 2 data; whether they engage in covered data transactions with covered persons or countries of concern; and how such data is marketed, particularly with respect to current or recent former employees or contractors, or former senior officials, of the United States government, including the military and U.S. Intelligence Community. NSD recognizes that individuals and companies may need to take steps to determine whether the DSP's prohibitions and restrictions apply to their activities, and to implement changes to their existing policies or to implement new policies and processes to

comply. These steps may vary greatly depending on the existing structure and commercial activities of the entities subject to the DSP, but could include revising or creating new internal policies and processes, identifying data flows, changing vendors or suppliers, adjusting employee roles or responsibilities, deploying new security requirements, and revising existing contracts. There are two key effective dates associated with the DSP: April 8, 2025 and October 6, 2025. Starting April 8, 2025, entities and individuals are required to comply with the DSP's prohibitions and restrictions, and with all other provisions of the DSP with the exception of the affirmative obligations of subpart J (related to due diligence and audit requirements for restricted transactions), § 202.1103 (related to reporting requirements for certain restricted transactions), and § 202.1104 (related to reports on rejected prohibited transactions). Starting October 6, 2025, entities and individuals must comply with subpart J and §§ 202.1103 and 202.1104. These effective dates remain in force. However, consistent with the Executive's Article II authority to exercise enforcement discretion, NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (e.g., individuals and companies) additional time to continue implementing the necessary changes to comply with the DSP and provide additional opportunities for the public to engage with NSD on DSP-related inquiries. Specifically, NSD will not prioritize civil enforcement actions against any person for violations of the DSP that occur from April 8 through July 8, 2025 so long as the person is engaging in good faith efforts to comply with or come into compliance with the DSP during that time. This policy aims to allow the private sector to focus its resources and efforts on promptly coming into compliance and to allow NSD to prioritize its resources on facilitating compliance. At the same time, during this 90-day period, NSD will pursue penalties and other enforcement actions as appropriate for egregious, willful violations. This policy does not limit NSD's authority and discretion to pursue civil enforcement if such persons did not engage in good-faith efforts to comply with, or come into compliance with, the DSP. Examples of evidence of good-faith efforts may include:

- Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitute data brokerage;
- Reviewing internal datasets and datatypes to determine if they are potentially subject to DSP;
- Renegotiating vendor agreements or negotiating contracts with new vendors;
- Transferring products and services to new vendors;
- Conducting due diligence on potential new vendors;
- Negotiating contractual onward transfer provisions with foreign persons who are the counterparties to data brokerage transactions; 3
- Adjusting employee work locations, roles or responsibilities;
- Evaluating investments from countries of concern or covered persons;
- Renegotiating investment agreements with countries of concern or covered persons; or
- Implementing the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

In considering any civil enforcement, NSD may also favorably consider, consistent with NSD enforcement policies, the extent to which a U.S. person voluntarily cooperated with any NSD inquiries. This policy does not restrict NSD's lawful authority and discretion to pursue

criminal enforcement in cases where individuals or entities willfully violate, attempt to violate, conspire to violate, cause a violation of, or engage in any action intended to evade or avoid the DSP's requirements.

During this 90-day period, NSD encourages the public to contact NSD at nsd.firs.datasecurity@usdoj.gov with informal inquires or information about the DSP and the guidance NSD has released. Although NSD may not be able to respond to every inquiry, NSD will use its best efforts to respond consistent with available resources, and any inquiries or information submitted may be used to develop and refine future guidance. Correspondingly, NSD discourages the submission of any formal requests for specific licenses or advisory opinions during this 90-day period: Although requests for specific licenses or advisory opinions during this 90-day period can be submitted, NSD will not review or adjudicate those submissions during the 90-day period (absent an emergency or imminent threat to public safety or national security).

At the end of this 90-day period, individuals and entities should be in full compliance with the DSP and should expect NSD to pursue appropriate enforcement with respect to any violations. This Implementation and Enforcement Policy does not create any privileges, benefits, or rights, substantive or procedural, enforceable at law or in equity by any individual, organization, party, or witness in any administrative, civil, criminal, or other matter

NSD Data Security Program - Implementation and Enforcement Policy for First 90 Days - 04112025

APPENDIX E— ***CONSUMER ALERT*** ATTORNEY GENERAL RAOUL URGES RESIDENTS TO TAKE PRECAUTIONS TO AVOID TAX IDENTITY THEFT WHEN FILING TAX RETURNS ABOUT BACK-TO-SCHOOL SCAMS
March 11, 2025

Chicago — As the income tax filing deadline approaches, Attorney General Kwame Raoul today issued guidance to help Illinois residents safely file tax returns and urged people to exercise caution before providing personally identifying and financial information online.

"Unfortunately, bad actors stand ready to take advantage of consumers during tax season," Raoul said. "The best way to prevent fraud from taking place is to protect your personal information. I am encouraging people to access free resources to help them make informed choices as we approach the tax filing deadline."

Tuesday, April 15 is the last day most taxpayers can file their income taxes, and Attorney General Raoul is reminding people to be on the lookout for scam tax preparers and to thoroughly review documents before signing them. Raoul encourages consumers who need a tax preparer to seek assistance from reputable sources, such as the Taxpayer Advocate Service provided by the Internal Revenue Service (IRS). Additionally, the IRS offers qualified consumers access to free tax filing services. Raoul also says consumers should check tax preparers' qualifications and browse the IRS Free File Online Lookup Tool.

The Attorney General is reminding individuals to review documents, including those that require electronic signatures, as scam tax preparers can use e-signatures to attempt to deceptively sign tax documents and consent forms, or to justify charges for expensive unnecessary services and high fees. Raoul encourages people to ask questions if they do not understand something, and go elsewhere for assistance with filing if the tax preparer will not or cannot provide an answer.

Attorney General Raoul is also warning individuals to protect their personal information, as scammers can steal that information and use it to file tax returns early and even receive any tax refunds owed to the consumer. Victims, especially those who do not file taxes regularly, sometimes do not realize they have been scammed until they receive a written notice from the IRS informing them a duplicate return has been filed. People should immediately contact the IRS if they receive any IRS notices that do not apply to them.

Raoul offered tips to help consumers avoid becoming a victim of tax identity theft:

- Do your research before selecting a tax preparer. Make sure you are using a reputable tax preparer before handing over your personal information. Search online for free, in-person tax preparation assistance.
- The U.S. Department of Veterans Affairs also offers tips and resources for veterans filing tax returns.
- Protect your Social Security number (SSN). Don't give out your SSN unless there is a good reason for doing so and only if you know to whom you are providing it.

- Apply for and use an Identity Protection PIN. This six-digit number confirms your identity and prevents someone else from filing a tax return using your Social Security number. Once you receive your PIN, you must provide it each year when you file your federal tax returns. Visit IRS.gov for more information.
- Report any suspicious or threatening IRS mail, phone, email or social media correspondence to the Treasury Inspector General for Tax Administration online or by calling 800-366-4484.
- Check that any correspondence claiming to be sent from the IRS, has a phone number and contact information that actually belongs to the IRS.
- Suspected IRS phone scams can also be reported by visiting the Federal Trade Commission's website and listing "IRS Telephone Scam" in the comments.
- Report unsolicited emails claiming to be from the IRS, or an IRS-related service like the Electronic Federal Tax Payment System, to the IRS by emailing phishing@irs.gov.
- Contact the Attorney General's Identity Theft Unit by calling 866-999-5630.

According to the IRS, tax professionals who engage in remote transactions have been especially vulnerable to identity thieves posing as potential clients who send an attachment that they claim includes their tax information. Once the tax preparer clicks on the URL or opens the attachment, malware secretly downloads onto their computers, giving thieves access to passwords for client accounts or remote access to the computers themselves. Tax professionals have a responsibility to protect taxpayer data by securing their network, and Raoul urges tax professionals to learn how to safeguard that data by reviewing IRS guidance.

Individuals who need to report a complaint involving a tax preparer or tax refund anticipation product should visit the Attorney General's website or call the Attorney General's Consumer Fraud hotlines:

1-800-386-5438 (Chicago)
1-800-243-0618 (Springfield)
1-800-243-0607 (Carbondale)

https://illinoisattorneygeneral.gov/news/story/consumer-alert-attorney-general-raoul-urges-residents-to-take-precautions-to-avoid-tax-identity-theft-when-filing-tax-returns

APPENDIX F- ***CONSUMER ALERT*** ATTORNEY GENERAL RAOUL WARNS ABOUT BACK-TO-SCHOOL SCAMS
August 06, 2025

Chicago – With summer almost over and the start of school just around the corner, Attorney General Kwame Raoul is warning Illinoisans to be wary of back-to-school scammers trying to take advantage of students and their families. Back-to-school scammers, like all scammers, try to trick consumers into paying for services or items that they will likely never receive or sharing personal data that scammers can use to steal consumers' identities.

"Consumers should not let the stress and expense of returning to the classroom keep them from doing their due diligence when buying school supplies online, getting test prep help or filling out scholarship applications," Raoul said. "My office provides advice and resources to help people avoid identity theft and assist those who think their information may have been compromised. I encourage people to visit my office's website for more details."

Attorney General Raoul encourages consumers shopping for school supplies online to consider the following smart shopping tips:

- Use trusted sites rather than shopping through a search engine. Fraudulent websites may look like the real thing and may even have a similar website address. Double check to ensure you have typed in the right website address. Remember that just because a website is at the top of the search results doesn't mean it's the official website. Scammers may use ads and sponsored links to trick you into visiting their websites.
- Price check popular items through multiple retailers to help determine if a deal is too good to be true. Comparison shopping before making a purchase can help you avoid overpaying for low-quality items.
- Read reviews of unfamiliar businesses to find out from other users if the website could be a scam. More focused information can also be found by doing an online search of a company or seller's name along with the words "scam" or "review."
- Pay for online purchases with a credit card so that the transaction is protected by the Fair Credit Billing Act. Liability for fraudulent charges on credit cards is generally limited. Paying with a debit card or gift card may not offer such safeguards.
- Exercise caution when entering personal information. Never give out private information – such as your Social Security number, payment information, usernames or passwords – in an email, text message or a pop-up chat box.
- Read the fine print. Be on the lookout for hidden costs or purchases that could register you for monthly charges.
- Research "buy now, pay later" plans and other payment deferral mechanisms. Deferrals allow shoppers to make a purchase right away but defer payment over a period of weeks or months. Some "zero-interest" offers include interest and additional fees, which can

spike if there is a missed payment, and even impact a consumer's credit score. Read the privacy policies and monitor the payment schedule if you decide to enter into such a plan.

Consumers should be careful of school supply giveaways. Remember to research on any website that requests your email or other personal information claiming you will be entered to win a prize. If you receive an email, social media message, text, or phone call claiming you won a contest that you do not remember entering, it is probably a scam.

Scammers can also prey on your generosity. If you are donating money to help students receive school supplies, be careful when paying through a credit card reader, a QR code, or a peer-to-peer app. Scammers may say they are charging you one amount, but may actually charge your app hundreds or thousands of dollars when you're not looking. Treat these payments as if they are final, because most of the time they are.

Attorney General Raoul further cautions consumers that now is a time to be vigilant for test-prep and financial aid scams. Be careful of companies that:

- Send unsolicited emails, texts, calls or social media messages informing you that you won a scholarship you don't remember applying for. Such messages are likely a scam.
- Claim to be able to give you access to a special or secret scholarship database for a fee.
- Claim to be able to give you exclusive access to a school, scholarship or the federal government.
- Charge money to fill out your Federal Application for Federal Student Aid (FAFSA). FAFSAs can be done for free on the Federal Student Aid website, and contact centers can help walk you through the steps.
- Require an upfront fee to submit your scholarship application.
- Guarantee that you will receive a certain amount of aid or will win a scholarship.
- Request your FSA ID, Social Security number, bank account or credit card information.
- Use high-pressure tactics or limited-time offers to trick you into acting faster than you are comfortable with.

If you think you have been a victim of a scam, you can file a complaint on the Attorney General's website or call the office's Consumer Fraud Hotlines:

1-800-386-5438 (Chicago)
1-800-243-0618 (Springfield)
1-800-243-0607 (Carbondale)
1-866-310-8398 (Spanish-language hotline)

https://illinoisattorneygeneral.gov/news/story/consumer-alert-attorney-general-raoul-warns-about-back-to-school-scams

APPENDIX G- ***CONSUMER ALERT* ATTORNEY GENERAL RAOUL URGES CONSUMERS TO DO THEIR HOLIDAY SHOPPING WITH CAUTION**
November 26, 2025

Chicago – Ahead of Black Friday and Cyber Monday, Attorney General Kwame Raoul is reminding Illinois residents to exercise caution when shopping both online and in person.

Raoul is also reminding shoppers to review the U.S. Consumer Product Safety Commission's (CPSC) recent recalls and product safety warnings before shopping this holiday season. The CPSC's up-to-date list highlights hundreds of items with recalls or safety warnings, including toys, clothing, furniture and household items. He is also encouraging shoppers to research the safety and packaging of items for signs of tampering or damage before purchasing.

"Black Friday and Cyber Monday are two of the biggest shopping days of the year, but shoppers should be careful to avoid scams or unsafe products in their rush to chase down the best deal," Raoul said. "My office provides advice and free resources to help avoid scams while shopping for loved ones. I encourage all Illinois consumers to take their time when making purchases and follow our tips for safe shopping this holiday season."

Attorney General Raoul encourages people to consider the following recommendations before shopping online this holiday season:

- **Research "buy now, pay later" plans and other payment deferral mechanisms.** Deferrals allow shoppers to make a purchase right away but defer payment over a period of weeks or months. Some "zero-interest" offers include interest and additional fees, which can spike if there is a missed payment, and even impact a consumer's credit score. Read the privacy policies and monitor the payment schedule if you decide to enter into such a plan.
- **Avoid fake websites. Fraudulent websites may look like the real thing and may even have a similar website address. Double check to ensure you have typed in the right website address. Remember that just because a website is at the top of the search results doesn't mean it's the official website.** Scammers may use ads, sponsored links, or social media promotions to trick you into visiting their look-alike websites and buying items that will never be delivered.
- **Read reviews if you are shopping on an unfamiliar website. More focused information can also be found by doing an online search of a company or seller's name along with the words "scam" or "review."**
- **Be careful when clicking on links that were sent to your phone or email from suspicious or unfamiliar sources. Never give a third-party remote access to your computer or download a company's software just to make a purchase. These may be "phishing" or "smishing" scams to trick you into going to a fake website or installing a virus on your device.**
- **Never give out private information – such as your Social Security number, payment information, usernames or passwords in an email, text message or a pop-up chat box.**

- **Be aware of "drop shippers."** Drop shippers don't own their inventory and only act as an intermediary between the consumer and a manufacturer. Dishonest drop shippers may try to trick you into believing they are the manufacturer, charge you extra fees, or send counterfeit goods or poor-quality goods – if you receive anything at all.
- **Always pay with a credit card.** Transactions paid with a credit card generally limit your liability for fraudulent charges. Paying by debit card, prepaid cards, gift cards and cash do not offer the same safeguards. When possible, use services such as Apple or Google Pay, which allow you to pay without providing your actual credit card number. If an actual credit card number is required, visit your credit card App or check with your issuer to see if a temporary one-time-use credit card is available.
- **Be wary if an online retailer or website does not accept credit card payments and requires that you pay by wire transfer, money order, gift card or cryptocurrency.**
- **Be extremely careful when sending peer-to-peer payments through apps such as Zelle, PayPal, Venmo and Cash App. Most peer-to-peer apps are designed so you can pay people or businesses you know, not people or businesses you are unfamiliar with. As a result, almost all the consumer protections associated with credit cards do not exist with P2P Apps.** Double check the recipient's name, phone number, email address or profile photo before hitting the send/confirmation button. Avoid sending or receiving money from anyone you don't know or trust. If you are sending money to someone for the first time, have them send you a "request" before you send the money.
- **Use multifactor authentication or two-step verification when possible.**
- **Read the fine print to make sure there aren't hidden costs or obligations that could sign you up for recurring charges, like a subscription or a membership.**
- **Ensure you receive a delivery date.** If a seller doesn't promise a timeline to ship in their ad, they must ship your order within 30 days of receiving your name, address and payment, unless they explain delays and give you the option to cancel and receive a refund.
- **Sign up for free fraud alerts from your bank or credit card.**
- **Use different usernames and passwords for all your accounts, keeping the password in a secure place and changing the password every six months.**
- **Don't rush. It can be tempting to move quickly to try to score good deals in the frenzy of the holiday sale season. Scammers count on perceived pressure to convince us to do things we otherwise wouldn't, such as sharing personal information. Taking time to evaluate offers can save you from getting stuck with a payment plan that charges high interest rates or fees, and c**omparison shopping before making a purchase can help you avoid overpaying for low-quality items.
- **Buy gift cards from behind a counter, or a retailer, and check to ensure they are untampered with—or that the PIN number on the back is not exposed—to avoid gift card draining scams. Thieves sometimes steal gift cards from store shelves to copy the card number and then put the cards back on the shelf. After purchase, the consumer's funds that were loaded onto the card are then immediately used by the scammer, leaving the gift card drained. Also be wary of gift cards purchased from third parties and online auction sites.**
- **Report counterfeit, unsafe, or stolen goods on third-party seller websites:** the Federal Trade Commission's Integrity, Notification, and Fairness in Online Retail Marketplaces ("INFORM") for Consumers Act and the Illinois INFORM Consumers Act requires

online marketplaces to protect consumers from counterfeit, unsafe, and stolen goods by verifying the identity of high-volume third-party sellers on their platforms. Recently, the FTC obtained a settlement against Temu for failing to provide a mechanism for reporting suspicious marketplace activity on the platform. If there is no mechanism to report such activity for high-volume sellers on these platforms, file a complaint with our Office or the FTC.

https://illinoisattorneygeneral.gov/news/story/consumer-alert-attorney-general-raoul-urges-consumers-to-do-their-holiday-shopping-with-caution