



**OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS**

**KWAME RAOUL
ATTORNEY GENERAL**

December 20, 2024

**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 2024.

Thank you.

Best Regards,

Matthew W. Van Hise

**Matthew W. Van Hise, CIPP/US
Chief Privacy Officer
Task Force Chair
Chief, Privacy & Data Security Unit
Assistant Attorney General
Illinois Attorney General's Office**

Enclosure: 2024 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 20, 2024

CONTENTS

- I. Task Force Background
 - Membership of the Task Force
- II. Part I: Protection of SSNs in the Public Record
 - Identity Protection Act: Identity-Protection Policy
 - Protecting Social Security Numbers – New Developments
- III. Part II: SSNs as Internal Identifiers
 - Minimizing the Use of Social Security Numbers
 - i. Illinois Attorney General’s Office – 2nd Annual Cyber Symposium
- IV. Task Force Appointments & Updates
- V. Conclusion
- VI. Appendix A: Template Identity-Protection Policy
- VII. Appendix B: Template Statement of Purpose(s)
- VIII. Appendix C: Executive Order on Preventing Access to Americans’ Bulk Sensitive Personal Data . . .
- IX. Appendix D: Illinois Attorney General’s Office Announces Virtual Cyber Symposium

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 – **Representative Dan Ugaste, Representative Randy Frese**
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jacqueline Collins, *Awaiting Additional Member Appointment Confirmation***
- Two members representing the Senate, appointed by the Minority Leader of the Senate - ***Awaiting Additional Member Appointment Confirmation, Awaiting Additional Member Appointment Confirmation***
- One member representing the Office of the Attorney General – **Matthew W. Van Hise, Task Force Chair**

- One member representing the Office of the Secretary of State – **Micah Miller**
- One member representing the Office of the Governor – ***Awaiting Member Appointment Confirmation***
- 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 – **Katelyn Nassin**
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- 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: Chief Privacy Officer Matthew W. Van Hise
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:

The continued updating of laws and regulations is necessary to combat identity fraud and theft, and safeguard personal information, while also ensuring users have access to personal information when necessary and appropriate.

On February 28, 2024, President Biden issued Executive Order 14117 (Order) which authorizes the Attorney General to protect against large-scale transfer of Americans’ personal data to countries of concern and provides safeguards around other activities that can give those countries access to sensitive data. The Order focuses on personal and sensitive information, including genomic data, biometric data, personal health data, geolocation data, financial data, and certain kinds of personally identifiable information, including SSNs. Bad actors can use this data for nefarious purposes as well pass that data on to other data brokers which can result in intrusive surveillance, scams, blackmail, and other violations of privacy.

As part of the Order, President Biden sought to restrict and limit “countries of concern” from purchasing bulk sensitive from data brokers. Sales of bulk sensitive data or governmental-related data by US persons would be prohibited if the transaction has been deemed an unacceptable security risk. The Order further orders a review of the infrastructure to transport data to countries of concern, including the submarine cables used to better secure data.

Additionally, the Order requires the Department of Defense, Health and Human Services, Veteran Affairs, and the National Science Foundation to consider steps to protect sensitive personal health data and human genomic data and submit a report within one year. The Consumer Financial Protection Bureau (CFPB) was also encouraged to review the risks related to the routine collection, dissemination, etc. of sensitive and governmental data and address it within their existing legal authority or through rulemaking.

Consistent with its obligation under the Order, on December 13, 2024, the CFPB proposed a rule that would amend the Regulation V that would implement the Fair Credit Reporting Act’s definition of consumer reports and consumer reporting agencies to add additional protections on sensitive customer information as defined by FCRA.¹ This would limit the sale of personal identifiers, including Social Security Numbers, by data brokers.

As of 2024, 20 states have enacted comprehensive privacy laws that take additional steps to protect the privacy and security of sensitive personal information. State legislatures may use the Order and the CFPB’s new rulemaking in consideration of any state legislation advancements.

(Executive Order on Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern – Appendix C)

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. To successfully minimize the use and exposure of SSNs, entities must understand how and why SSNs have been collected and where they are stored. With an SSN inventory and classification system they can ensure proper access, retention, and disposal of sensitive information.

¹ Protecting Americans From Harmful Data Broker Practices, 89 Fed. Reg. 240 (Dec. 13, 2024) (to be codified at 12 C.F.R. Part 1022) <https://www.federalregister.gov/d/2024-28690>

In an effort to raise awareness on current best practices of data security, data privacy, organizational preparation and response, and threats posed by artificial intelligence, the Illinois Attorney General's Office hosted its second annual cybersecurity symposium. Over two days, members of various government organizations and private cybersecurity experts discussed topics geared towards Illinois agencies but also was attended by local business owners and non-profit organizations.

Panelists discussed the importance of data minimization and reducing the amount of sensitive data collected. Topics included the consideration of the use of automated tools or other strategies to analyze how data is being collected and to categorize the location of sensitive information held. These steps help ensure data is being appropriately safeguarded. Once the data is categorized and classified, panelists explained how this simplifies the process to ensure retention for only as long as necessary and confirm that sensitive data is disposed of consistent with state and federal law.

The symposium also covered topics focused on emerging trends in cybersecurity, including technologies which agencies can utilize to prevent intrusions, as well as steps they can proactively take to minimize the effects of cyber-attacks. Identifying where information, like SSNs are held and how that information is collected, will help entities increase security and limit exposure from a security incident. Analyzing SSNs through their lifecycle at an organization or agency will help identify where SSNs may be replaced by less sensitive information.

(Attorney General Raoul Offers Virtual Cybersecurity Symposium – Appendix D)

TASK FORCE APPOINTMENTS & UPDATES

The Task Force awaits calendar year 2024 Appointment and Confirmations for the following currently vacant membership seats:

- (1) Member representing the House of Representatives, Appointed by the Speaker of the House;
- (1) Member representing the Senate, Appointed by the President of the Senate;
- (2) Members representing the Senate, Appointed by the Minority Leader of the Senate; and
- (1) Member representing the Office of the Governor;

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 not²:

² 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,

- 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

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.

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.

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 – Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

By the authority vested in me as President by the Constitution and the laws of the United States of America, 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.](#)) (NEA), and [section 301 of title 3, United States Code](#),

I, JOSEPH R. BIDEN JR., President of the United States of America, hereby expand the scope of the national emergency declared in [Executive Order 13873](#) of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in [Executive Order 14034](#) of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). The continuing effort of certain countries of concern to access Americans' sensitive personal data and United States Government-related data constitutes an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security and foreign policy of the United States. Access to Americans' bulk sensitive personal data or United States Government-related data increases the ability of countries of concern to engage in a wide range of malicious activities. Countries of concern can rely on advanced technologies, including artificial intelligence (AI), to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States. Countries of concern can also use access to bulk data sets to fuel the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data and exacerbating the national security and foreign policy threats. In addition, access to some categories of sensitive personal data linked to populations and locations associated with the Federal Government—including the military—regardless of volume, can be used to reveal insights about those populations and locations that threaten national security. The growing exploitation of Americans' sensitive personal data threatens the development of an international technology ecosystem that protects our security, privacy, and human rights.

Accordingly, to address this threat and to take further steps with respect to the national emergency declared in [Executive Order 13873](#), it is hereby ordered that:

Section 1 . Policy. It is the policy of the United States to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States. At the same time, the United States continues to support open, global, interoperable, reliable, and secure flows of data across borders, as well as maintaining vital consumer, economic, scientific, and trade relationships that the United States has with other countries.

The continuing effort by countries of concern to access Americans' bulk sensitive personal data and United States Government-related data threatens the national security and foreign policy of the United States. Such countries' governments may seek to access and use sensitive personal data in a manner that is not in accordance with democratic values, safeguards for privacy, and other human rights and freedoms. Such countries' approach stands in sharp contrast to the practices of democracies with respect to sensitive personal data and principles reflected in the

Organisation for Economic Co-operation and Development Declaration on Government Access to Personal Data Held by Private Sector Entities. Unrestricted transfers of Americans' bulk sensitive personal data and United States Government-related data to such countries of concern may therefore enable them to exploit such data for a variety of nefarious purposes, including to engage in malicious cyber-enabled activities. Countries of concern can use their access to Americans' bulk sensitive personal data and United States Government-related data to track and build profiles on United States individuals, including Federal employees and contractors, for illicit purposes, including blackmail and espionage. Access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements poses particular and unacceptable risks to our national security given that these arrangements often can provide countries of concern with direct and unfettered access to Americans' bulk sensitive personal data. Countries of concern can use access to United States persons' bulk sensitive personal data and United States Government-related data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

This risk of access to Americans' bulk sensitive personal data and United States Government-related data is not limited to direct access by countries of concern. Entities owned by, and entities or individuals controlled by or subject to the jurisdiction or direction of, a country of concern may enable the government of a country of concern to indirectly access such data. For example, a country of concern may have cyber, national security, or intelligence laws that, without sufficient legal safeguards, obligate such entities and individuals to provide that country's intelligence services access to Americans' bulk sensitive personal data and United States Government-related data.

These risks may be exacerbated when countries of concern use bulk sensitive personal data to develop AI capabilities and algorithms that, in turn, enable the use of large datasets in increasingly sophisticated and effective ways to the detriment of United States national security. Countries of concern can use AI to target United States persons for espionage or blackmail by, for example, recognizing patterns across multiple unrelated datasets to identify potential individuals whose links to the Federal Government would be otherwise obscured in a single dataset.

While aspects of this threat have been addressed in previous executive actions, such as [Executive Order 13694](#) of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended, additional steps need to be taken to address this threat.

At the same time, the United States is committed to promoting an open, global, interoperable, reliable, and secure Internet; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows required to enable international commerce and trade; and facilitating open investment. To ensure that the United States continues to meet these important policy objectives, this order does not authorize the imposition of generalized data

localization requirements to store Americans' bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process Americans' bulk sensitive personal data or United States Government-related data within the United States. This order also does not broadly prohibit United States persons from conducting commercial transactions, including exchanging financial and other data as part of the sale of commercial goods and services, with entities and individuals located in or subject to the control, direction, or jurisdiction of countries of concern, or impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific, and trade relationships that the United States has with other countries. In addition, my Administration has made commitments to increase public access to the results of taxpayer-funded scientific research, the sharing and interoperability of electronic health information, and patient access to their data. The national security restrictions established in this order are specific, carefully calibrated actions to minimize the risks associated with access to bulk sensitive personal data and United States Government-related data by countries of concern while minimizing disruption to commercial activity. This order shall be implemented consistent with these policy objectives, including by tailoring any regulations issued and actions taken pursuant to this order to address the national security threat posed by access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern.

Sec. 2 . *Prohibited and Restricted Transactions.* (a) To assist in addressing the national emergency described in this order, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, shall 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 further defined by regulations issued by the Attorney General pursuant to this section;

(ii) is a member of a class of transactions that has been determined by the Attorney General, in regulations issued by the Attorney General pursuant to this section, 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 this order;

(iii) was initiated, is pending, or will be completed after the effective date of the regulations issued by the Attorney General pursuant to this section;

(iv) does not qualify for an exemption provided in, or is not authorized by a license issued pursuant to, the regulations issued by the Attorney General pursuant to this section; and

(v) is not, as defined by regulations issued by the Attorney General pursuant to this section, ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory

or regulatory requirements, including any regulations, guidance, or orders implementing those requirements.

(b) The Attorney General, in consultation with the heads of relevant agencies, is authorized to take such actions, including the promulgation of rules and regulations, and to employ all other powers granted to the President by IEEPA, as may be necessary or appropriate to carry out the purposes of this order. Executive departments and agencies (agencies) are directed to take all appropriate measures within their authority to implement the provisions of this order.

(c) Within 180 days of the date of this order, the Attorney General, in coordination with the Secretary of Homeland Security, and in consultation with the heads of relevant agencies, shall publish the proposed rule described in subsection (a) of this section for notice and comment. This proposed rule shall:

(i) identify classes of transactions that meet the criteria specified in subsection (a)(ii) of this section that are to be prohibited (prohibited transactions);

(ii) identify classes of transactions that meet the criteria specified in subsection (a)(ii) of this section and for which the Attorney General determines that security requirements established by the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency, in accordance with the process described in subsection (d) of this section, adequately mitigate the risk of access by countries of concern or covered persons to bulk sensitive personal data or United States Government-related data (restricted transactions);

(iii) identify, with the concurrence of the Secretary of State and the Secretary of Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of this order;

(iv) establish, as appropriate, mechanisms to provide additional clarity to persons affected by this order and any regulations implementing this order (including by designations of covered persons and licensing decisions);

(v) establish a process to issue (including to modify or rescind), in concurrence with the Secretary of State, the Secretary of Commerce, and the Secretary of Homeland Security, and in consultation with the heads of other relevant agencies, as appropriate, licenses authorizing transactions that would otherwise be prohibited transactions or restricted transactions;

(vi) further define the terms identified in section 7 of this order and any other terms used in this order or any regulations implementing this order;

(vii) address, as appropriate, coordination with other United States Government entities, such as the Committee on Foreign Investment in the United States, the Office of Foreign Assets Control within the Department of the Treasury, the Bureau of Industry and Security within the Department of Commerce, and other entities implementing relevant programs, including those implementing [Executive Order 13873](#); [Executive Order 14034](#); and [Executive Order 13913](#) of

April 4, 2020 (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector); and

(viii) address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts.

(d) The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall, in coordination with the Attorney General and in consultation with the heads of relevant agencies, propose, seek public comment on, and publish security requirements that address the unacceptable risk posed by restricted transactions, as identified by the Attorney General pursuant to this section. These requirements shall be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology.

(i) The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall, in coordination with the Attorney General, issue any interpretive guidance regarding the security requirements.

(ii) The Attorney General shall, in coordination with the Secretary of Homeland Security acting through the Director of the Cybersecurity and Infrastructure Security Agency, issue enforcement guidance regarding the security requirements.

(e) The Secretary of Homeland Security, in coordination with the Attorney General, is hereby authorized to take such actions, including promulgating rules, regulations, standards, and requirements; issuing interpretive guidance; and employing all other powers granted to the President by IEEPA as may be necessary to carry out the purposes described in subsection (d) of this section.

(f) In exercising the authority delegated in subsection (b) of this section, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, may, in addition to the rulemaking directed in subsection (c) of this section, propose one or more regulations to further implement this section, including to identify additional classes of prohibited transactions; to identify additional classes of restricted transactions; with the concurrence of the Secretary of State and the Secretary of Commerce, to identify new or remove existing countries of concern and, as appropriate, classes of covered persons for the purposes of this order; and to establish a mechanism for the Attorney General to monitor whether restricted transactions comply with the security requirements established under subsection (d) of this section.

(g) Any proposed regulations implementing this section:

(i) shall reflect consideration of the nature of the class of transaction involving bulk sensitive personal data or United States Government-related data, the volume of bulk sensitive personal data involved in the transaction, and other factors, as appropriate;

(ii) shall establish thresholds and due diligence requirements for entities to use in assessing whether a transaction is a prohibited transaction or a restricted transaction;

(iii) shall not establish generalized data localization requirements to store bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process bulk sensitive personal data or United States Government-related data within the United States;

(iv) shall account for any legal obligations applicable to the United States Government relating to public access to the results of taxpayer-funded scientific research, the sharing and interoperability of electronic health information, and patient access to their data; and

(v) shall not address transactions to the extent that they involve types of human 'omic data other than human genomic data before the submission of the report described in section 6 of this order.

(h) The prohibitions promulgated pursuant to this section apply except to the extent provided by law, including by statute or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of the applicable regulations directed by this order.

(i) Any transaction or other activity that has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions promulgated pursuant to this section is prohibited.

(j) Any conspiracy formed to violate any of the prohibitions promulgated pursuant to this section is prohibited.

(k) In regulations issued by the Attorney General under this section, the Attorney General may prohibit United States persons from knowingly directing transactions if such transactions would be prohibited transactions under regulations issued pursuant to this order if engaged in by a United States person.

(l) The Attorney General may, consistent with applicable law, redelegate any of the authorities conferred on the Attorney General pursuant to this section within the Department of Justice. The Secretary of Homeland Security may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary of Homeland Security pursuant to this section within the Department of Homeland Security.

(m) The Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, is hereby authorized to submit recurring and final reports to the Congress related to this order, consistent with section 401(c) of the NEA ([50 U.S.C. 1641\(c\)](#)) and section 204(c) of IEEPA ([50 U.S.C. 1703\(c\)](#)).

Sec. 3 . *Protecting Sensitive Personal Data.* (a) Access to bulk sensitive personal data and United States Government-related data by countries of concern can be enabled through the transmission of data via network infrastructure that is subject to the jurisdiction or control of countries of concern. The risk of access to this data by countries of concern can be, and sometime is, exacerbated where the data transits a submarine cable that is owned or operated by

persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that connects to the United States and terminates in the jurisdiction of a country of concern. Additionally, the same risk of access by a country of concern is further exacerbated in instances where a submarine cable is designed, built, and operated for the express purpose of transferring data, including bulk sensitive personal data or United States Government-related data, to a specific data center located in a foreign jurisdiction. To address this threat, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee) shall, to the extent consistent with its existing authority and applicable law:

(i) prioritize, for purposes of and in reliance on the process set forth in section 6 of [Executive Order 13913](#), the initiation of reviews of existing licenses for submarine cable systems that are owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that terminate in the jurisdiction of a country of concern;

(ii) issue policy guidance, in consultation with the Committee's Advisors as defined in section 3(d) of [Executive Order 13913](#), regarding the Committee's reviews of license applications and existing licenses, including the assessment of third-party risks regarding access to data by countries of concern; and

(iii) address, on an ongoing basis, the national security and law enforcement risks related to access by countries of concern to bulk sensitive personal data described in this order that may be presented by any new application or existing license reviewed by the Committee to land or operate a submarine cable system, including by updating the Memorandum of Understanding required under section 11 of [Executive Order 13913](#) and by revising the Committee's standard mitigation measures, with the approval of the Committee's Advisors, which may include, as appropriate, any of the security requirements contemplated by section 2(d) of this order.

(b) Entities in the United States healthcare market can access bulk sensitive personal data, including personal health data and human genomic data, through partnerships and agreements with United States healthcare providers and research institutions. Even if such data is anonymized, pseudonymized, or de-identified, advances in technology, combined with access by countries of concern to large data sets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data, which may reveal the exploitable health information of United States persons. While the United States supports open scientific data and sample sharing to accelerate research and development through international cooperation and collaboration, the following additional steps must be taken to protect United States persons' sensitive personal health data and human genomic data from the threat identified in this order:

(i) The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall consider taking steps, including issuing regulations, guidance, or orders, as appropriate and consistent with the legal authorities authorizing relevant Federal assistance programs, to prohibit the provision of assistance that enables access by countries of concern or covered persons to United States persons' bulk sensitive personal data, including personal health data and human genomic data, or to impose mitigation measures with respect to such assistance, which may be consistent with the

security requirements adopted under section 2(d) of this order, on the recipients of Federal assistance to address this threat. The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall, in consultation with each other, develop and publish guidance to assist United States research entities in ensuring protection of their bulk sensitive personal data.

(ii) Within 1 year of the date of this order, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall jointly submit a report to the President through the Assistant to the President for National Security Affairs (APNSA) detailing their progress in implementing this subsection.

(c) Entities in the data brokerage industry enable access to bulk sensitive personal data and United States Government-related data by countries of concern and covered persons. These entities pose a particular risk of contributing to the national emergency described in this order because they routinely engage in the collection, assembly, evaluation, and dissemination of bulk sensitive personal data and of the subset of United States Government-related data regarding United States consumers. The Director of the Consumer Financial Protection Bureau (CFPB) is encouraged to consider taking steps, consistent with CFPB's existing legal authorities, to address this aspect of the threat and to enhance compliance with Federal consumer protection law, including by continuing to pursue the rulemaking proposals that CFPB identified at the September 2023 Small Business Advisory Panel for Consumer Reporting Rulemaking.

Sec. 4 . *Assessing the National Security Risks Arising from Prior Transfers of United States Persons' Bulk Sensitive Personal Data.* Within 120 days of the effective date of the regulations issued pursuant to section 2(c) of this order, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, in consultation with the heads of relevant agencies, shall recommend to the APNSA appropriate actions to detect, assess, and mitigate national security risks arising from prior transfers of United States persons' bulk sensitive personal data to countries of concern. Within 150 days of the effective date of the regulations issued pursuant to section 2(c) of this order, the APNSA shall review these recommendations and, as appropriate, consult with the Attorney General, the Secretary of Homeland Security, and the heads of relevant agencies on implementing the recommendations consistent with applicable law.

Sec. 5 . *Report to the President.* (a) Within 1 year of the effective date of the regulations issued pursuant to section 2(c) of this order, the Attorney General, in consultation with the Secretary of State, the Secretary of the Treasury, the Secretary of Commerce, and the Secretary of Homeland Security, shall submit a report to the President through the APNSA assessing, to the extent practicable:

(i) the effectiveness of the measures imposed under this order in addressing threats to the national security of the United States described in this order; and

(ii) the economic impact of the implementation of this order, including on the international competitiveness of United States industry.

(b) In preparing the report described in subsection (a) of this section, the Attorney General shall solicit and consider public comments concerning the economic impact of this order.

Sec. 6 . *Assessing Risks Associated with Human 'omic Data.* Within 120 days of the date of this order, the APNSA, the Assistant to the President and Director of the Domestic Policy Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Pandemic Preparedness and Response Policy, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, the Director of the National Science Foundation, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation, shall submit a report to the President, through the APNSA, assessing the risks and benefits of regulating transactions involving types of human 'omic data other than human genomic data, such as human proteomic data, human epigenomic data, and human metabolomic data, and recommending the extent to which such transactions should be regulated pursuant to section 2 of this order. This report and recommendation shall consider the risks to United States persons and national security, as well as the economic and scientific costs of regulating transactions that provide countries of concern or covered persons access to these data types.

Sec. 7 . *Definitions.* For purposes of this order:

(a) The term “access” means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information technology systems, cloud computing platforms, networks, security systems, equipment, or software.

(b) The term “bulk” means an amount of sensitive personal data that meets or exceeds a threshold over a set period of time, as specified in regulations issued by the Attorney General pursuant to section 2 of this order.

(c) The term “country of concern” means any foreign government that, as determined by the Attorney General pursuant to section 2(c)(iii) or 2(f) of this order, has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons, and poses a significant risk of exploiting bulk sensitive personal data or United States Government-related data to the detriment of the national security of the United States or the security and safety of United States persons, as specified in regulations issued by the Attorney General pursuant to section 2 of this order.

(d) The term “covered person” means an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern; a foreign person who is an employee or contractor of such an entity; a foreign person who is an employee or contractor of a country of concern; a foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or any person designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, as acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or as knowingly causing or directing, directly or indirectly, a violation of this order or any regulations implementing this order.

(e) The term “covered personal identifiers” means, as determined by the Attorney General in regulations issued pursuant to section 2 of this order, specifically listed classes of personally identifiable data that are reasonably linked to an individual, and that—whether in combination with each other, with other sensitive personal data, or with other data that is disclosed by a transacting party pursuant to the transaction and that makes the personally identifiable data exploitable by a country of concern—could be used to identify an individual from a data set or link data across multiple data sets to an individual. The term “covered personal identifiers” does not include:

(i) demographic or contact data that is linked only to another piece of demographic or contact data (such as first and last name, birth date, birthplace, zip code, residential street or postal address, phone number, and email address and similar public account identifiers); or

(ii) a network-based identifier, account-authentication data, or call-detail data that is linked only to another network-based identifier, account- authentication data, or call-detail data for the provision of telecommunications, networking, or similar services.

(f) The term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(g) The term “foreign person” means any person that is not a United States person.

(h) The term “human genomic data” refers to data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a cell.

(i) The term “human 'omic data” means data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomic data, or metabolomic data, as further defined by regulations issued by the Attorney General pursuant to section 2 of this order, which may be informed by the report described in section 6 of this order.

(j) The term “person” means an individual or entity.

(k) The term “relevant agencies” means the Department of State, the Department of the Treasury, the Department of Defense, the Department of Commerce, the Department of Health and Human Services, the Office of the United States Trade Representative, the Office of the Director of National Intelligence, the Office of the National Cyber Director, the Office of Management and Budget, the Federal Trade Commission, the Federal Communications Commission, and any other agency or office that the Attorney General determines appropriate.

(l) The term “sensitive personal data” means, to the extent consistent with applicable law including sections 203(b)(1) and (b)(3) of IEEPA, covered personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof, as further defined in regulations issued by the Attorney General pursuant to section 2 of this order, and that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any

identifiable United States individual or to a discrete and identifiable group of United States individuals. The term “sensitive personal data” does not include:

(i) data that is a matter of public record, such as court records or other government records, that is lawfully and generally available to the public;

(ii) personal communications that are within the scope of section 203(b)(1) of IEEPA; or

(iii) information or informational materials within the scope of section 203(b)(3) of IEEPA.

(m) The term “United States Government-related data” means sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security and that:

(i) a transacting party identifies as being linked or linkable to categories of current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of this order;

(ii) is linked to categories of data that could be used to identify current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of this order; or

(iii) is linked or linkable to certain sensitive locations, the geographical areas of which will be specified publicly, that are controlled by the Federal Government, including the military.

(n) The term “United States person” means 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.

Sec. 8 . General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) Nothing in this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.

(c) Any disputes that may arise among agencies during the consultation processes described in this order may be resolved pursuant to the interagency process described in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System), or any successor document.

(d) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

<https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related>

**APPENDIX D: ATTORNEY GENERAL RAOUL OFFERS VIRTUAL
CYBERSECURITY SYMPOSIUM
June 13, 2024**

Free Event Will Feature Speakers from the FBI, FTC, U.S. Secret Service and More
Chicago – Attorney General Kwame Raoul is encouraging business owners, government officials, directors of non-profit organizations and others interested in cybersecurity to register for the Illinois Attorney General’s Office’s 2nd Annual Cybersecurity Symposium.

The free, virtual event will take place on Monday, June 17, from 9:15 a.m. to 5:15 p.m. and Tuesday, June 18, from 9:30 a.m. to 11:15 a.m. The symposium will feature speakers from the Federal Bureau of Investigation (FBI), Federal Trade Commission, Federal Commerce Commission, Cybersecurity and Infrastructure Security Agency, the U.S. Secret Service and the Attorney General’s Office.

“In today’s environment of cyber threats, it’s not a matter of if, but when your organization will be attacked,” Raoul said. “It’s important to know how to protect yourself and how to respond after an attack has occurred. I am proud to offer this resource, and I encourage anyone who wants to learn more about cybersecurity to register for it. I thank all of our law enforcement and regulatory partners who have volunteered to bring their expertise to this symposium.”

The event will feature an evaluation of the current cyberthreat landscape, as well as sessions focused on data security, organizational preparation and response, cybersecurity audits and threats posed by artificial intelligence, among other topics.

“Though cyber crime is an unfortunate fact of life in our increasingly digital world, awareness is a powerful tool in the fight against it,” said FBI Special Agent in Charge Robert W. “Wes” Wheeler, Jr. “The FBI is proud to join with our partners to share cybersecurity best practices with our local community.” Wheeler is scheduled to be a speaker at the event.