HOUSE COMMITTEE ON
NATURAL RESOURCES
CHAIRMAN BRUCE WESTERMAN

To:	Subcommittee on Oversight and Investigations Republican Members
From:	Subcommittee on Oversight and Investigations staff, Michelle Lane and Thomas Knecht x6-8747
Date:	Wednesday, June 7, 2023
Subject:	Oversight Hearing on "*Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State-Sponsored Cyber Actors*"

The Subcommittee on Oversight and Investigations will hold an oversight hearing on "*Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State-Sponsored Cyber Actors*" on **Wednesday, June 7, 2023, at 2:00 p.m. EDT in 1324 Longworth House Office Building.**

Member offices are requested to notify Sophia Varnasidis by 4:30 p.m. on June 5, 2023, if their Member intends to participate in the hearing.

I. KEY MESSAGES

- All U.S. government agencies must prioritize cybersecurity, including the Department of the Interior (DOI), because cyberattacks can disrupt government operations and threaten America's national security and owned assets.

- Cybersecurity is an ongoing process and agencies should continually work to identify, protect, and detect cybersecurity threats. This includes identifying system weaknesses and implementing best practices.

- U.S. government agencies are increasingly subject to threats from state-sponsored actors, notably China.

- The DOI Office of Inspector General (OIG) and the Government Accountability Office (GAO) recently issued separate reports on cybersecurity weaknesses at DOI that expose the vulnerability of DOI's information systems, DOI's assets, and America's offshore energy infrastructure.

- The cybersecurity weaknesses at DOI threaten America's energy sector and national security.

II. WITNESSES

- Panel 1
  - **The Hon. Mark Greenblatt**, Inspector General, U.S. Department of the Interior, Washington, DC
  - **Ms. Marisol Cruz Cain**, Director, Information Technology and Cybersecurity, Government Accountability Office, Washington, DC
- Panel 2
  - **Mr. Brian Cavanaugh**, Fellow for Cybersecurity, Intelligence, and Homeland Security, Heritage Foundation
  - **Mr. Dean Cheng**, Senior Advisor, China Program, United States Institute of Peace, Washington, DC
  - **Dr. T. Charles Clancy Sr.**, Sr. VP & GM, MITRE Labs & Chief Futurist, The MITRE Corp., McLean, VA
  - **Ms. Rhea Siers**, Senior Advisor (Cyber Risk), Teneo, Washington, DC

III. BACKGROUND

Congress, leading executive agencies, and the last several Presidents have all recognized the ongoing importance of securing America's information systems, data, and users. The ever-evolving technology and pervasive threats are reflected in the legislation, agency standards, and executive orders aimed to promote America's cybersecurity. While nation-states are launching increasingly sophisticated cyberattacks to further their strategic and geopolitical priorities, many U.S. government agencies do not adequately prioritize cybersecurity, leaving American assets, data, technology, systems, and users exposed to attack. Recent reports from the OIG and GAO highlight significant cybersecurity lapses at DOI that undermine U.S. national, cyber, and economic security.

A. Cybersecurity Basics

Cybersecurity refers to the security of devices, infrastructure, data, and users of computers, computer networks, information and communications technology, virtual systems, or computer-enabled control of physical components.[1] Federal agencies are responsible for collecting, processing, storing, and disposing of a large amount of digital information related to individuals, businesses, and sensitive matters.[2] Cybersecurity includes managing that data, and the systems using the data, in a secure way.[3] It is an ongoing process that requires agency planning, implementing processes, and conducting programming.[4]

[1] *See generally* Chris Jaikaran, CONG. RESEARCH SERV., IF10559, *Cybersecurity: A Primer* (Dec. 8, 2022), https://sgp.fas.org/crs/misc/IF10559.pdf [hereinafter *Cybersecurity Primer*].
[2] Chris Jaikaran, CONG. RESEARCH SERV., R46926, *Federal Cybersecurity: Background and Issues for Congress* 5 (Sep. 29, 2021), https://crsreports.congress.gov/product/pdf/R/R46926.
[3] *Id.*
[4] *Id.*

Confidentiality, *integrity*, and *availability* are widely viewed by industry experts as the three main components to information, system, and device security.[5] A fourth key component to information, system, and device security is *authentication*.[6]

Government officials and agencies can reduce cybersecurity threats by ensuring the confidentiality, integrity, and availability of information and systems. The authentication of users is an additional means to protect data and devices. U.S. government agencies must prioritize ensuring cybersecurity because attacks can disrupt government operations and threaten America's national security.

	Confidentiality	**Integrity**	**Availability**	**Authentication**
Definition	Data is only known to and used by authorized parties.	Data and systems aren't altered without authorization; device accurately reflects data and usage.	Data, systems, and device are available to authorized parties when they choose.	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.[7]
Example of compromise or attack	Data breach.	Data manipulation.	Ransomware.	Guessing weak passwords.
Tool to prevent compromise, attack, and/or disruption	Encryption.	Hashing.	Tool to support data availability: backing up data.	Password protection, multi-factor authentication, biometric, token.
Further explanation	Encryption is the process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it.[8]	Hashing is a process that generates a value or values from a string of text using a mathematical formula.[9]	Ransomware is a type of malware (malicious software) that locks a victim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransom to the attacker.[10]	Token-based authentication is a form of two-factor authentication, meaning users must supply two unique factors when logging in. The first factor is something the user knows, like a password or PIN. The second factor is provided by an authenticator, a hardware or software token with a code that changes randomly, usually every sixty seconds.[11]

[5] *Cybersecurity Primer*, *supra* note 1.
[6] *Id.*
[7] NIST, *Authentication*, https://csrc.nist.gov/glossary/term/authentication (last visited May 31, 2023).
[8] GOOGLE, *What is encryption?*, https://cloud.google.com/learn/what-is-encryption (last visited May 31, 2023).
[9] GOOGLE, *Hashing: Definition*, https://support.google.com/google-ads/answer/9004449?hl=en (last visited May 31, 2023).
[10] IBM, *What is ransomware?*, https://www.ibm.com/topics/ransomware (last visited May 31, 2023).
[11] AT&T BUSINESS, *What is Token Authentication?*, https://www.business.att.com/learn/what-is-token-authentication.html (May 31, 2023).

B. Nation-State Cyber Threats and Notable State-Sponsored Cyberattacks on U.S. Government Agencies

While cyberattacks are often associated with independent hackers exploiting vulnerabilities for personal financial gain,[12] nation-states are launching increasingly sophisticated cyberattacks to further their strategic and geopolitical priorities.[13] Recent events have led industry leaders to describe cyberweapon deployment as the dawn of a new age of conflict.[14] Nation-state actors engage in intellectual property theft, espionage, surveillance, credential theft, destructive attacks, and more.[15] America's intelligence agencies view the greatest nation-state cyber threats as the People's Republic of China (PRC), Russia, North Korea, and Iran.[16] For over a decade, these nation-state actors have directed various cybersecurity attacks against U.S. government agencies.

2009: Suspected North Korean DDoS attacks against the U.S. & South Korea

In July 2009, shortly after Independence Day, an unknown assailant attacked more than 20 governmental and commercial Internet websites in the United States with distributed denial of service (DDoS) attacks.[17] Some of these websites attacked included the White House, Department of Justice, Department of State, Department of Defense, and commercial websites sites such as Yahoo and Amazon. South Korean government websites – including the National Congress, Ministry of Defense, and National Intelligence Service – were also attacked.[18] While there were significant signs of North Korea leading the attacks, the attacker masked their activities, preventing investigators from fully revealing the program or locating the route infecting the servers.[19]

2013-2017: Proxies for Iranian Government Attack U.S. Government Agencies

From 2013 to 2017, cyber criminals associated with the Mabna Institute, an Iranian company, targeted intellectual property and other data from 144 U.S. universities, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the state of Hawaii, and the state of Indiana, and various companies and organizations outside the United States.[20] The attacks were conducted by private sector contractors who engaged in computer intrusion, wire fraud, and data theft at the behest of the government of Iran and the Iranian Revolutionary Guard Corps, the

---

[12] *See* Joe Tidy, *Ransomware: Should paying hacker ransoms be illegal?*, BBC NEWS (May 20, 2021), https://www.bbc.com/news/technology-57173096.
[13] Microsoft, *Microsoft Digital Defense Report 2022* 30 (2002) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.
[14] *Id*. at 31.
[15] *Id*. at 33.
[16] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
[17] Motohiro Tsuchiya, *Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States*, in *Cybersecurity: Public Sector Threats and Responses*, 55-62 (Kim Andreasson ed., 2012), https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/40114/9781439846636.pdf?sequence=1&isAllowed=y.
[18] *Id*.
[19] *Id*.
[20] Catherine A. Theohary, CONG. RESEARCH SERV., IF11406, *Iranian Offensive Cyberattack Capabilities* (Jan. 13, 2020) https://www.parstimes.com/history/crsirancyber-jan20.pdf.

military force that oversees Iran's offensive cyberactivity.[21]

The Department of Justice indicted nine Iranians for these incidents in March 2018.[22] As alleged in the indictment, the men were involved in a scheme to obtain unauthorized access to computer systems, steal proprietary data from those systems, and sell that stolen data to the Iranian government and various Iranian universities.[23]

2012-2020: Russian Hackers Attack Energy Sector and Infiltrate Information Networks at the Treasury and Commerce Departments in SolarWinds Hack

From 2012-2018, Russian nationals working for the Russian government conducted various cyberattacks against the global energy sector.[24] In total, the hacking campaigns targeted thousands of computers, at hundreds of companies and organizations, in approximately 135 countries.[25] The operation included: (a) damaging critical energy infrastructure that caused two separate emergency shutdowns at a targeted facility; (b) hacking the computers of a U.S. company that managed similar critical infrastructure entities in the United States; and (c) targeting and compromising the computers of hundreds of entities related to the energy sector worldwide to provide the Russian government the ability to disrupt and damage computer systems at a future time of its choosing.[26]

Separately, in 2020, the Trump administration declared that Russian hackers, likely working at the behest of a Russian intelligence agency, broke into a range of key government information networks, including at the Treasury and Commerce Departments, and had free access to their email systems.[27] It was described as one of the most sophisticated, and perhaps among the largest attacks on federal systems in recent history as hackers pierced automatic updates of outside products from SolarWinds, an IT company, to distribute malware for exfiltrating information from U.S. government agency systems. [28] Other victims included FireEye, a computer security firm that first raised the alarm about the Russian campaign after its own systems were pierced, and the National Telecommunications and Information Administration, a Commerce agency that helps determine internet policy and sets standards for the import/export of technology considered a national security risk.[29] As of February 17, 2021, nine federal agencies and approximately 100 private sector companies were known to have been compromised by the SolarWinds attack.[30]

---

[21] *Id*.
[22] FBI, *Most Wanted: Iranian Mabna Hackers* (Mar. 23, 2018), https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers.
[23] *Id*.
[24] DEP'T OF JUSTICE, *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide* (Mar. 24, 2022), https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.
[25] *Id*.
[26] *Id*.
[27] David E. Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (Dec. 13, 2020), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html.
[28] Jaikaran, *supra* note 2.
[29] *Id*.
[30] *Id*. at 3.

2014-2015: China Steals Personal Information of Four Million Federal Employees

In 2015, the United States Office of Personnel Management (OPM), the agency responsible for managing the federal government's civilian workforce, announced that attackers exfiltrated personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals from OPM records.[31] The hackers conducted two separate attacks, in 2014 and 2015, and were linked to the government of the PRC. U.S. officials described the data breach as among the largest known thefts of government data in history.[32]

Among the sensitive data that was exfiltrated were millions of SF-86 forms, which contain personal identifiable information gathered in background checks for people seeking government security clearances, and records of millions of people's fingerprints.[33] The compromised databases included information such as fingerprint data, Social Security Numbers, financial records, IT system credentials, and even performance evaluations.[34] According to the Federal Bureau of Investigation (FBI), the information taken in large data thefts allow the PRC to identify targets for espionage campaigns and program artificial intelligence systems.[35]

The intelligence and counterintelligence value of the stolen background information is significant. Then-Director of the FBI James Comey described the data breach as a very big deal from a national security and counterintelligence perspective because it is a "treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government."[36] Likewise, as described by former Central Intelligence Agency Director Michael Hayden, "there's no fixing it" as the damage is likely irreparable with the information "available to the Chinese until the people represented by the information age off."[37]

The breach was not a surprise to those monitoring the ongoing cybersecurity vulnerabilities at OPM. Since 2205, the OPM Inspector General issued warnings that the information maintained by OPM was vulnerable to hackers and, since 2007, fundamental factors of the OPM's information security system were rated as a *significant deficiency* or worse.[38]

---

[31] U.S. OFF. OF PERS. MGMT., *Cybersecurity Resource Center*, https://www.opm.gov/cybersecurity/ (last visited May 31, 2023).
[32] Devlin Barrett et al., *U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say*, WALL ST. J. (June 5, 2015) https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.
[33] Josh Fruhlinger, *The OPM hack explained: Bad security practices meet China's Captain America*, CSO (Feb. 12, 2020), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.
[34] Jaikaran, *supra* note 2.
[35] Christopher Wray, Director, FBI, Remarks at the Hudson Institute Video Event: China's Attempt to Influence U.S. Institutions, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States* (July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-andthe-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.
[36] Julie Hirschfield Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.
[37] FEDSCOOP, *Impact of OPM breach could last more than 40 years* (July 10, 2015), https://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community/#:~:text=%E2%80%9CI%20don't%20think%20there,There's%20no%20fixing%20it.%E2%80%9D.
[38] OFF. OF INSPECTOR GEN., U.S. OFFICE OF PERS. MGMT, No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014), https://www.oversight.gov/sites/default/files/oig-reports/OPM/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016_0.pdf.

Despite the annual and repeated warnings from the OPM Inspector General for nearly a decade, OPM failed to implement the necessary cybersecurity measures. The cybersecurity failures allowed hackers to gain access to OPM's systems, the hackers entrenched into those systems, and accessed the agency's Active Directory to gain root access, and spread malware through other systems. The victims were millions of federal employees and the security of the American public.

May 2023: Chinese Government Hacking Group Targets U.S. Systems in Guam

In May 2023, the United States National Security Agency, the Cybersecurity and Infrastructure Security Agency (CISA), and the FBI, issued a issued a joint Cybersecurity Advisory regarding a cluster of activity of interest associated with a PRC state-sponsored cyber actor.[39] The actor, also called "Volt Typhoon," is a Chinese government hacking group focused on espionage and information gathering.[40] Volt Typhoon used "built-in network administration tools" to evade detection and perform its objectives.[41] The tactics, techniques, and procedures included blending in with normal Windows system and network activities to avoid endpoint detection and triggering response products that would alert on the introduction of third-party applications to the host.[42] Volt Typhoon also intentionally limited the amount of activity captured in default logging configurations to further reduce the likelihood of detection.[43]

Volt Typhoon installed the evasive computer code in telecommunications systems in Guam and other areas in the United States. The activity in Guam is noteworthy because "Guam, with its Pacific ports and vast American air base, would be a centerpiece of any American military response" to an invasion or blockade of Taiwan or American assets in the Indo-Pacific region.[44] The PRC's targeting of Guam takes increased importance given their ongoing efforts to gain influence over U.S. territories and the Freely Associated States in the Pacific.[45]

C. Cybersecurity Vulnerabilities at the Department of the Interior

In separate reports, the OIG and GAO recently identified significant cybersecurity vulnerabilities at DOI. It is imperative for DOI to implement the OIG and GAO recommendations and make a renewed commitment to cybersecurity to protect its assets, help ensure energy security, and promote national security.

---

[39] NAT'L SEC. AGENCY et al., *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection* (May 24, 2023) https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF.

[40] MICROSOFT THREAT INTELLIGENCE, *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques* (May 24, 2023), https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

[41] NAT'L SEC. AGENCY, *supra* note 55.

[42] *Id*.

[43] *Id*.

[44] David E. Sanger, *Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?*, N.Y. TIMES (May 24, 2023), https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html?campaign_id=190&emc=edit_ufn_20230524&instance_id=93396&nl=from-the-times&regi_id=210828370&segment_id=133817&te=1&user_id=979bb1ccbe6564c599925c6e448cad29.

[45] *See generally* STAFF OF THE S. COMM. ON INDIAN AND INSULAR AFFAIRS, H. COMM. ON NATURAL RESOURCES, 118TH CONG., *Memo. for Oversight Hearing Preserving U.S. Interests in the Indo-Pacific: Examining How U.S. Engagement Counters Chinese Influence in the Region* (May 16, 2023), https://naturalresources.house.gov/uploadedfiles/hearing_memo__sub_on_iia_ov_hrg_on_the_indo_pacific_051623.pdf.

OIG: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk

In January 2023, the OIG issued a report highlighting fundamental weaknesses in DOI's password complexity requirements.[46] The OIG found that DOI's password management and enforcement controls were not effective enough to prevent a malicious actor from gaining unauthorized access to DOI's computer systems by capturing and cracking user passwords.[47] The OIG compared the password vulnerabilities at DOI to the Colonial Pipeline ransomware attack in which one stolen password resulted in cybercriminals effectively shut down half the country's fuel supply chain by using a stolen password leaked online.[48]

Notably, the OIG cracked 18,174 of 85,944 – or 21 percent of active user passwords, including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees.[49] Other OIG Findings:[50]

- DOI did not consistently implement multifactor authentication, including for 89 percent of its High Value Assets (assets that could have serious impacts to the Department's ability to conduct business if compromised), which left these systems vulnerable to password compromising attacks.

- DOI's password complexity requirements were outdated and ineffective, allowing users to select easy-to-crack passwords (e.g., Changeme$12345, Polar_bear65, Nationalparks2014!).

    - 4.75 percent of all active user account passwords were based on the word "password." In the first 90 minutes of testing, the IG cracked the passwords for 16% of DOI's user accounts.

- DOI's password complexity requirements implicitly allowed unrelated staff to use the same inherently weak passwords – meaning there was not a rule in place to prevent this practice.
    - The most commonly reused password (Password-1234) were used on 478 unique active accounts.
    - 5 of the 10 most reused passwords at DOI included a variation of "password" combined with "1234"; a combination that met the Department's requirements even though it is not difficult to crack.

[46] OFF. OF INSPECTOR GEN., U.S. DEP'T OF THE INTERIOR, *P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk* (Jan. 2023), https://www.doioig.gov/sites/default/files/2021-migration/Final%20Inspection%20Report_DOI%20Password_Public.pdf?emci=66664715-fd90-ed11-9d7b-00224832e811&emdi=7f680e01-0491-ed11-9d7b-00224832e811&ceid=9011
[47] *Id*. at 1.
[48] *Id*.
[49] *Id*. at 10.
[50] *Id*. at 12-23.

- DOI did not timely disable inactive (unused) accounts or enforce password age limits, which left more than 6,000 additional active accounts vulnerable to attack.

Considering the significant password vulnerabilities, the OIG made recommendations to increase DOI's password security, implement multi-factor authentication, align with best practices and standards, prioritize controls for senior employees or accounts with elevated privileges, prohibit oft-repeated passwords, and implement unique and complex temporary passwords and passphrases.[51]

GAO: Offshore Oil and Gas – DOI Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure

In October 2022, GAO issued a report that found DOI's offshore oil and gas infrastructure faces significant and increasing cybersecurity risks in the form of threat actors, vulnerabilities, and potential impacts.[52] GAO criticized DOI's Bureau of Safety and Environmental Enforcement (BSEE) for having long recognized cybersecurity risks, dating back to at least 2015, but failing to address the concerns.[53] Indeed, BSEE has taken few actions to address cybersecurity risks to the more than 1,600 oil and gas facilities and structures on the Outer Continental Shelf.[54]

As a result of failures by BSEE and DOI, America's offshore infrastructure is particularly vulnerable to state actors who may conduct a cyberattack to disrupt (a) oil and gas production, (b) oil and gas transmission, and/or (c) energy supplies and markets. GAO found that successful cyberattacks against offshore oil and gas infrastructure could have potentially severe effects on safety, the environment, and the economy[55] and a successful cyberattack/technology failure would be catastrophic, resulting in death and negative impacts to energy supplies, markets, and the economy.[56]

GAO recommended the BSEE Director should immediately develop and implement a strategy to guide the development of its most recent cybersecurity initiative.[57] The strategy should contain (1) a risk assessment; (2) objectives, activities, and performance measures; (3) roles, responsibilities, and coordination; and (4) identification of needed resources and investments.[58]

D. The Regulatory Landscape of Cybersecurity Compliance: Legislation, Agency Standards, and Executive Orders

Over the last several decades, Congress, executive branch agencies, and successive Presidents have all recognized the ongoing importance of protecting U.S. government assets from cybersecurity threats.

---

[51] *Id*.
[52] U.S. GOV'T ACCOUNTABILITY OFF., *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure* 13 (Oct. 2022), https://www.gao.gov/assets/gao-23-105789.pdf.
[53] *Id*. at Highlights.
[54] *Id*. at 25.
[55] *Id*. at 17.
[56] *Id*. at 19.
[57] *Id*. at 26.
[58] *Id*.

Three federal statutes establish the main principles under which U.S. government agencies secure information technology (IT) equipment, networks, data, and users:

- *The Privacy Act of 1974*: Governs how U.S. government agencies may collect and retain an individual's records and how agencies may, or may not, disclose that information to another party. The statute impacts how agencies store, process, and dispose of information held in IT systems.[59]

- *The Federal Information Technology Acquisition Reform Act of 2014* (FITARA): Requires chief information officers to review and approve IT acquisitions for their agency and exercise governance and oversight over IT planning, programming, budgeting, and execution activities. While not primarily a cybersecurity law, it also requires chief information officers to work with the Office of Management and Budget (OMB) to identify and improve the risk management of IT investments.[60]

- *Federal Information Security Modernization Act of 2014* (FISMA): Updated requirements for each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.[61]
    - Establishes roles, responsibilities, standards, and guidelines for federal agencies to manage IT security and risks.[62]
    - FISMA strengthens the use of continuous monitoring in systems, increases focus on the agencies for compliance and reporting that is more focused on the issues caused by security incidents.

The executive branch agencies charged with protecting America's information systems regularly issue guidance and procedures on cybersecurity.

- OMB provides broad, strategic directions to agencies on cybersecurity.

- The National Institute of Standards and Technology (NIST) issues standards and guidance that U.S. government agencies are required to follow.[63] Notable standards developed by NIST include security measures for IT systems,[64] a risk management framework,[65] and a catalog of security and privacy requirements agencies must implement for their IT systems.[66]

---

[59] Jaikaran, *supra* note 2.
[60] *Id*.
[61] NAT'L INST. OF STANDARDS AND TECH., *NIST Risk Management Framework*, https://csrc.nist.gov/projects/risk-management/fisma-background (last visited May 31, 2023).
[62] Jaikaran, *supra* note 2.
[63] 15 U.S.C. §278g–3 and 40 U.S.C. §11331.
[64] NAT'L INST. OF STANDARDS AND TECH., FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[65] NAT'L INST. OF STANDARDS AND TECH., SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (Dec. 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.
[66] NAT'L INST. OF STANDARDS AND TECH., SP 800-53, *Security and Privacy Controls for Information Systems and*

- The Department of Homeland Security (DHS) provides operational assistance to help agencies implement laws and guidance[67] and, acting through CISA, a DHS agency, DHS issues Binding Operational Directives (BODs), which are compulsory directions for federal agencies to implement for the protection and security of federal information and IT systems. Notable DHS BODs:
    - *BOD 18-02, Securing High Value Assets*: Requires agencies to identify and report their high-value IT assets to DHS, allowing DHS to assess the security of those assets, and mitigate any vulnerabilities that DHS finds within 30 days.[68]
    - *BOD 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems*: Requires agencies to review and mitigate DHS-found vulnerabilities on internet accessible IT systems within 30 days of notification.[69]
    - *BOD 20-01, Develop and Publish a Vulnerability Disclosure Policy*: Requires agencies to create and publish policies on how the public can identify vulnerabilities in federal IT systems and alert the agency of the potential risk.[70]

Presidents have highlighted the growing importance of cybersecurity to America's vital interests through recent executive orders:

- *Executive Order 13556, Controlled Unclassified Information*: Established an open and uniform program for managing unclassified information requiring safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. [71]

- *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*: Directed U.S. Government agencies to address their cyber risk management framework and standardize these efforts in line with the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. Also empowered the Secretary of Homeland Security to act as the nation's key coordinator for all aspects of critical infrastructure security, including cybersecurity. [72]

Organizations, (Sep. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[67] Jaikaran, *supra* note 2
[68] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, BOD 18-02, *Securing High Value Assets* (May 7, 2018), https://cyber.dhs.gov/bod/18-02/.
[69] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems* (Apr. 29, 2019), https://cyber.dhs.gov/bod/19-02/.
[70] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy* (Sep. 2, 2020), https://cyber.dhs.gov/bod/20-01/.
[71] EXEC. ORDER NO. 13556, 75 F.R. 68675 (Nov. 4, 2010), https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information.
[72] EXEC. ORDER NO. 13556, 82 F.R. 22391 (May 11, 2017), https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

- *Executive Order 13870, America's Cybersecurity Workforce*: Sought to promote the development of the U.S. government's cybersecurity workforce by enhancing the career mobility and supporting the development of cybersecurity staff in the executive branch.[73]

- *Executive Order 14028, Improving the Nation's Cybersecurity*: Required entities providing information and communications technology to the federal government to report to CISA when they discover a cyber incident on a product or service used by the government.[74]

IV. CONCLUSION

U.S. government agencies must prioritize ensuring cybersecurity because cyberattacks can disrupt government operations and threaten America's national security. Cybersecurity is an ongoing process and agencies should continually work to identify, protect, and detect cybersecurity threats. This includes identifying system weaknesses and implementing best practices. U.S. government agencies are increasingly subject to threats from state-sponsored actors, notably China.

Cybersecurity weaknesses at DOI that expose the vulnerability of DOI's information systems, DOI's assets, and America's offshore energy infrastructure. In doing so, the cybersecurity weaknesses at DOI threaten America's energy sector and national security. It is imperative that DOI implement recommendations to significantly increase password security requirements and better secure its cyber infrastructure, data, users, networks, information, communications technology, virtual systems, and computer-enabled control of physical components.

[73] EXEC. ORDER NO. 13870, 84 F.R. 20523 (May 2, 2019), https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce.
[74]EXEC. ORDER NO. 14028, 86 F.R. 26633 (May 12, 2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.