Cybersecurity: Bureau of Cyber Statistics

January 19, 2023

Congressional Research Service
https://crsreports.congress.gov
R47389

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47389

January 19, 2023

Chris Jaikaran
Specialist in Cybersecurity Policy

Cybersecurity: Bureau of Cyber Statistics

The scope and scale of cyberattacks against the United States have been difficult to catalog and quantify. Most observers recognize the frequency, severity, and diversity of such attacks as increasing. A lack of uniform data on the attacks stymies public policy debate and action.

Some government agencies and private companies already collect cyber incident information. Federal and state regulators may require certain entities to report when they experience certain types of attacks; and private cybersecurity companies collect data on incidents from their customers. However, the data are not centralized, standardized, or filtered for duplication. The variation of data and the number of different houses for those data limit the data's use to understand the scope and scale of cyberattacks.

In an effort to create a central repository of cyber incident data, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The act requires the Cybersecurity and Infrastructure Security Agency (CISA) to (1) engage in rulemaking to require private sector entities to report when they experience a cyberattack or pay a ransom; (2) enforce compliance with required reporting; and (3) disseminate analysis based on the information collected. CISA is currently working with stakeholders on developing a notice of proposed rulemaking.

A proposal that extends this concept is the Cyberspace Solarium Commission's (Commission) recommendation to create a Bureau of Cyber Statistics (BCS). The Commission's proposed BCS would be a federal statistical agency, and would collect, process, analyze, and distribute data on cybersecurity incidents, as well as the effects of those incidents. The proposal meets much of what CIRCIA intends. However, there is a key difference; the audience for BCS outputs would be policymakers and industry decisionmakers, as opposed to just the cybersecurity community. As a federal statistical agency, a BCS would produce objective analysis on cyber incidents to inform policymakers and industry, rather than collecting and analyzing data to serve a purpose or program for the agency itself. Additionally, as a federal statistical agency, a BCS would follow strict and rigorous methodologies for collecting and processing data, adding to its credibility.

Other federal statistical agencies include the U.S. Census Bureau, the Bureau of Justice Statistics, and the Bureau of Labor Statistics.

The Commission identified five distinct attributes for a BCS: (1) definition of cybersecurity metrics; (2) collection and aggregation of cyberattack data; (3) reporting mandates for incidents; (4) data and privacy protection; and (5) information exchange between academia and the private sector. While not specifically discussed by the Commission, an analytic capability would also be necessary for a BCS to develop useful products for policymakers and industry.

Recent proposals have advocated for establishing a BCS within CISA so that resources developed to implement CIRCIA can be leveraged. Despite the capabilities outlined by CIRCIA, CISA would still need to add others in order to achieve the full BCS capability.

Contents

Tables

Contacts

Introduction

This report provides information and analysis regarding the Cyberspace Solarium Commission's (Commission) 2020 recommendation to create a Bureau of Cyber Statistics (BCS).[1]

The Case for Improved Cybersecurity Statistics

Industry groups,[2] private companies,[3] and think tanks[4] have all attempted to catalogue and qualify the scope and scale of cyberattacks against the United States. It is widely accepted that with each passing year, such attacks become more diverse, more frequent, and more impactful.[5] Despite acceptance of these subjective statements as objective information, stakeholders have also recognized that the available data are insufficient to quantify and evaluate the totality of attacks and their effect on the nation.

Existing data on cyberattacks are held among many different public and private sources across federal and nonfederal entities. The data held by these entities are inconsistently reported, uneven in data object values (i.e., the information collected), and potentially redundant or duplicative. Furthermore, most of the available data only measure cyber risk input (e.g., the type of attack, indicators of compromise, and attribution). Data on attack responses and outcomes—measures that successfully defended the attack, the quantified loss from a successful attack (e.g., profit loss or down time), and changes to business operations from the attack—are rarely collected and analyzed. These challenges manifest for both government and industry in similar ways—the lack of data leads to weak analysis and poorly informed decisionmaking.

Some scholars argue that the lack of consistent and complete data inhibits policymakers from understanding the true scope and scale of cybersecurity risk and adopting appropriate policies to address those risks.[6] An analogy may be drawn to crime statistics: scholars argue that the standardized collection and analysis of national crime statistics have contributed to more evidence-based policymaking and positive policy shifts.[7]

Congress may experience challenges with insufficient data when evaluating annual agency budget requests or considering new authorizations for agencies. Members are asked to make choices on which programs to resource and determine how much investment will lead to a sufficient reduction in cybersecurity risk. Without independent information on risk management, Members must rely on agency claims and stakeholder input to determine which programs are funded and at what levels.

---

[1] Cyberspace Solarium Commission, "Final Report," *Recommendation 4.3*, March 2020, at https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf.

[2] FS-ISAC, "Navigating Cyber: 2021," report, 2021, at https://www.fsisac.com/hubfs/GIOReport2021/NavigatingCyber2021.pdf.

[3] Verizon, "DBIR: Data Breach Investigations Report," report, 2022, at https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf.

[4] Center for Strategic and International Studies, "Significant Cyber Incidents," website, May 2022, at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[5] CRS Video WVB00451, *2022 Issues & Policy - The Evolution of Cybersecurity Issues in the 117th Congress*, by Chris Jaikaran.

[6] Eileen Decker and Mieke Eoyang, "We Need Better Cybercrime Data," *Lawfare*, April 15, 2020, at https://www.lawfareblog.com/we-need-better-cybercrime-data.

[7] Ibid.

Industry also faces challenges from the lack of useful data. For instance, cybersecurity insurance has been touted as a market-driven tool to reduce cyber risk by pricing policies based on data related to risk exposure and mitigating measures.[8] However, the scarcity of historical information related to cyberattacks has complicated efforts to create accurate actuarial data.[9] Traditionally, insurers use data from previous claims as well as new data on emerging risks to develop price models for new policies, but in the absence of that information, these models have yet to be fully developed.[10]

Data for Risk Management

Risk is a function of *threats*, *vulnerabilities*, and *consequences*. Data on risk (e.g., the vulnerabilities that threat actors compromise and where an entity is vulnerable) are necessary to adequately assess management strategies' effectiveness. The Department of Homeland Security (DHS) has recognized the lack of comprehensive data on cybersecurity risk and has funded projects through its Science and Technology Directorate (S&T) related to improved information sharing (IMPACT)[11] and the economics of risk mitigation (CYRIE).[12] However, the limited scale of the pilot projects, low visibility into the work, and lack of mandates stymied project success and led to the end of government sponsorship.

Risk can be managed by *avoiding* it, *transferring* it, *controlling* it, and finally *accepting* it. One may also ignore risk, but that is not a management strategy. Cybersecurity insurance represents one way to mitigate risk—by *transferring* it. Companies may choose to *control* risk by buying goods and services to reduce their vulnerabilities or the consequences of an attack. However, without knowledge of the scope of risk and emerging trends, individual firms face similar challenges as Congress does when resourcing federal agencies—firms are uncertain which solutions are best to invest in and what investment levels may achieve desired effects.[13]

Additionally, insurers and firms are resigned to measure past risk and assume measures to control that risk will be sufficient in the future. However, cybersecurity risk is constantly evolving. Threat actors and cybersecurity companies continually learn from each other's tactics and strive to outpace the other's efforts. This active and dynamic environment means that past performance rarely provides a stable assumption upon which to base future investments.

[8] Department of Homeland Security/National Protection and Programs Directorate, *Cybersecurity Insurance Workshop Readout Report*, November 2012, https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf.

[9] National Research Council of the National Academies, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts of Issues*, 2014, at https://nap.nationalacademies.org/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic.

[10] Andrew Granato and Andy Polacek, "The Growth and Challenges of Cyber Insurance," *Chicago Fed Letter*, 2019, at https://www.chicagofed.org/-/media/publications/chicago-fed-letter/2019/cfl426-pdf.pdf?sc_lang=en.

[11] Department of Homeland Security, "Information Marketplace for Policy and Analysis of Cyber-Risk & Trust," website, October 25, 2021, at https://www.dhs.gov/science-and-technology/cybersecurity-impact.

[12] Department of Homeland Security, "Cyber Risk Economics," website, January 27, 2022, at https://www.dhs.gov/science-and-technology/cyrie.

[13] This assumes a firm is willing to invest in cybersecurity risk management. Many businesses may lack the knowledge, resources, or desire for major cybersecurity investments.

Review of the Bureau of Cyber Statistics Proposal

To provide better data to public policymakers and private decisionmakers, the Commission recommended in 2020 establishing a statistical agency to collect, process, analyze, and distribute data on cybersecurity incidents and their effects. This recommendation to create a Bureau of Cyber Statistics would inform efforts to create and amend cybersecurity policy and programs as well as complement other Commission recommendations, such as those related to informing national risk management and helping insurers create more accurate risk models.

The Commission based its BCS recommendation on the Bureau of Labor Statistics (BLS). Created in 1884, the BLS strives to provide objective and unadulterated data on the labor market for policymakers. To do this, BLS identified measures and metrics to track key matters (e.g., labor market activity, price changes, and unemployment), confidentially collects this data from respondents, and applies a transparent methodology to the data to create data products.[14] In turn, policymakers use BLS data (e.g., on employment, wage growth, and inflation)[15] and products like the Employment Cost Index[16] to understand the state of the national economy and inform policy decisions.

Similarly, a BCS could identify key measures of cyber incidents (e.g., common vulnerabilities exploited and costs associated with downtime and response) and develop data products (e.g., quantified attacks by critical infrastructure sector or region) to better understand national cyber risk.

To aid Congress in establishing a BCS, the Commission drafted model legislative text, which further elaborates on their recommendation.[17] The proposed BCS would be established within a federal agency.[18] The proposed BCS would be charged with:

- collecting and analyzing cybersecurity information (e.g., cyberattacks and crime) on a continual basis;
- compiling and publishing statistics from that cybersecurity information;
- coordinating with the National Institute of Standards and Technology (NIST) on standards and metrics for ensuring the reliability and validity of cybersecurity statistics;
- researching and innovating on methods to collect and analyze anonymized cybersecurity statistics;
- entering into agreements with other agencies, academia, and private companies to support the bureau's duties;
- providing the President, Congress, other federal agencies, the private sector, and the general public with cybersecurity statistics;

[14] Bureau of Labor Statistics, "About the U.S. Bureau of Labor Statistics," website, June 1, 2020, at https://www.bls.gov/bls/infohome.htm.

[15] Bureau of Labor Statistics, "Economic News Releases," website, April 4, 2022, at https://www.bls.gov/bls/newsrels.htm#major.

[16] Bureau of Labor Statistics, "Employment Cost Index News Release," *USDL-22-0712,* April 29, 2022, at https://www.bls.gov/news.release/eci.htm.

[17] Cyberspace Solarium Commission, "4.3 Establish a Bureau of Cyber Statistics," draft legislation, May 2022, at https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_4.3.pdf.

[18] The original proposal called for establishing a BCS within the Department of Commerce, but the recent draft text changed to place it within the CISA.

- liaising with state and local governments; and
- participating with other federal statistical agencies and conforming to such laws and regulations related to disclosure of federal statistical data.

In addition to these duties, the BCS would be authorized to develop specific statistics related to federal network operations, provide grants to state governments to help them submit data to the bureau, promulgate a rule requiring entities to report to the BCS after experiencing a cybersecurity incident, and issue fines to entities that violate the rule.

BCS as a Federal Statistical Agency

The legislative proposal highlights the importance of the proposed BCS as a federal statistical agency. A *federal statistical agency* is an executive branch organizational unit "whose principal function is to collect, compile, analyze, and disseminate information for such statistical uses as monitoring key economic and societal indicators ... evaluating programs, and conducting scientific research."[19]

Federal statistical agencies and recognized statistical units are subject to Office and Management and Budget (OMB) regulations pursuant to the Budget and Accounting Procedures Act of 1950 (P.L. 84-784),[20] the Paperwork Reduction Act of 1995 (P.L. 104-13),[21] and the Information Quality Act (P.L. 106-554)[22] such as Statistical Policy Directive 1.[23] Information collected and used by federal statistical agencies are also subject to confidentiality and use restrictions per the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA, P.L. 115-435).[24]

Federal Statistical Agency

A *federal statistical agency* (or *entity*) engages with *statistical activities* for a *statistical purpose.*

Statistical activities are defined as "the collection, compilation, processing, analysis, or dissemination of data for the purpose of describing or making estimates concerning the whole, or relevant groups or components within, the economy, society, or the natural environment, including the development of methods or resources that support those activities, such as measurement methods, models, statistical classifications, or sampling frames. Statistical activities implicitly but necessarily involve the design, editing, and storage of statistical data as instrumental to collection, compilation, processing, analysis, release, and dissemination of statistical information. Therefore, for clarity, this Directive explicitly refers to each of these as statistical activities."

Statistical purpose is defined as "the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support such purposes."

(Office of Management and Budget, "Statistical Policy Directive No. 1: Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units," 79 *Federal Register* 71614, December 2, 2014.)

[19] "Summary," in *Principles and Practices for a Federal Statistical Agency*, ed. Brian A. Harris-Kojetin and Constance F. Citro, 7th ed. (Washington, DC: The National Academies Press, 2021), p. 1.

[20] 31 U.S.C. §1104(d).

[21] 44 U.S.C. §3504(e).

[22] 44 U.S.C. §3502.

[23] Office of Management and Budget, "Statistical Policy Directive No. 1: Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units," 79 *Federal Register* 71610-71616, December 2, 2014.

[24] 44 U.S.C. §§3561-3583.

The collection and use of data by federal statistical agencies contrasts with that of other federal agencies. For instance, an industry regulator may require data from their regulated entity in order to inform future requirements on the industry. A federal statistical agency's work is not intended to impose a burden on industry or directly influence a program of that agency. Instead, a federal statistical agency's work is meant to inform policymakers and private sector entities. This is also different from the data collection that an agency engages in through normal business. For example, the Cybersecurity and Infrastructure Security Agency (CISA) collects data and produces products that are predominately used by the cybersecurity community. If, as recent proposals have advocated, a BCS is placed within CISA, then a portion of BCS work products would expand beyond the cybersecurity community to include non-cybersecurity policymakers and industries.

The conduct of federal statistical agencies in executing their activities is described in the principles of those agencies, and highlights how they are different from other executive branch agencies. According to the Committee on National Statistics, a federal statistical agency's work strives to be:

- relevant to policy issues and society;
- credible among data users and stakeholders;
- trusted among public and private providers of data;
- independent from political and external influence; and
- continually improving and innovating.[25]

Any federal agency may strive to meet these principles. However, specific programs or agency activities may face broad disagreement concerning relevancy, credibility and trust, or face significant political and external influence. This is where the rigorous methodological, data collection and processing methods that federal statistical agencies are beholden to serve to minimize criticism of products and increase public acceptance of them.

Cyber Incident Reporting Data Sources

The federal government receives reports of cybersecurity incidents and information related to cyber risk mitigation from a variety of sources—both voluntary and mandatory.

Table 1 provides a selected list of federal regulations requiring private sector entities to report cybersecurity specific incidents to federal entities, by sector.

Table 1. Selected Cyber Incident Reporting Requirements

Sector	Reporting Entity	Receiving Entity	Requirement	Authority
Federal Government	Federal Agencies	OMB, CISA, Congressional Committees	Report significant cyber incidents within OMB-prescribed time frames.	44 U.S.C. §3554 M-21-02
Communications	Undersea Cable Operators	FCC	Report outages related to submarine cables.	47 C.F.R. Part 4

[25] *Principles and Practices for a Federal Statistical Agency*, ed. Brian A. Harris-Kojetin and Constance F. Citro, 7th ed. (Washington, DC: The National Academies Press, 2021), p. 23.

Sector	Reporting Entity	Receiving Entity	Requirement	Authority
Defense Industrial Base	Defense Contractors	DOD	Analyze and report cyber incidents affecting covered defense information.	48 C.F.R. §§204, 212, 217, 252
Energy	Electricity Providers	FERC	Report cyber incidents if they have compromised or disrupted one or more tasks related to the reliability of energy distribution.	7 C.F.R. §1730 CIP-008-05
Financial Services	Financial Institutions	Financial Regulators	Report to regulators instances of unauthorized access to nonpublic customer information.	12 C.F.R. Part 30 12 C.F.R. Parts 208 and 225 12 C.F.R. Part 364 12 C.F.R. Parts 568 and 570
Health Care	Covered Health Care Institutions	HHS	Report losses of protected health information.	45 C.F.R. Part 160 and Subparts A and E of Part 164
Nuclear	Nuclear Licensees	NRC	Report cyber incidents that affect safety, security, emergency preparedness, or support systems of a nuclear site within one hour of discovery.	10 C.F.R. §73.77
Transportation	Pipeline Operators	TSA and CISA	Report actual or suspected cyberattacks that could impact industrial control systems, measurement or telemetry systems, or enterprise IT.	49 C.F.R. §114

Source: CRS analysis of the *Code of Federal Regulations*.

Notes: Office of Management and Budget (OMB), Memorandum on the Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (M-21-02). The following abbreviations appear in the table: Cybersecurity and Infrastructure Security Agency (CISA); Federal Communications Commission (FCC); Department of Defense (DOD); Federal Energy Regulatory Commission (FERC); Critical Infrastructure Protection Reliability Standard (CIP); Department of Health and Human Services (HHS); Nuclear Regulatory Commission (NRC); Transportation Security Agency (TSA); Information Technology (IT); Department of Education (ED); *U.S. Code* (U.S.C.); and *Code of Federal Regulations* (C.F.R.).
Depending on the financial institution, the financial regulator for cyber incident reporting may include the Federal Reserve System Board of Governors, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and state regulatory agencies.

Despite the existence of these reporting requirements, there is no comprehensive picture of national cybersecurity risk. First, not every critical infrastructure sector has a regulator that requires reporting from covered entities within the sector. The chemical, commercial facilities, critical manufacturing, dams, emergency services, food and agriculture, information technology, and water and wastewater system sectors do not have sector-specific cybersecurity incident reporting mandates.

Further, some sectors have incomplete mandates. For example, the communications sector's mandate only covers undersea cable disruptions; the transportation sector mandate only applies to

pipelines. These narrow remits arguably ignore some of the largest concerns in those sectors (i.e., internet service providers for the communications sector; aviation companies for transportation).

Second, while industry is required to make reports to a specific agency, there is rarely an obligation for one agency to further report that incident to another agency—let alone to a central agency for consolidated analysis.

A mechanism exists whereby information about cybersecurity risk can be shared: private sector entities may share cyber threat information amongst themselves through information sharing and analysis centers (ISAOs), the private sector may share information with CISA, and government agencies may share information amongst themselves at the Director of National Intelligence's Cyber Threat Intelligence Integration Center (CTIIC). However, participation in these types of information sharing programs has seen limited success.[26] Furthermore, there are still barriers to regular information sharing that inhibit government management of cybersecurity risk. For example, information classification standards and uncertainty about liability protections continue to impede information sharing.[27]

The disparate collection of data held across the federal government has led some in Congress to advocate for the implementation of another Commission recommendation—the proposed Joint Collaborative Environment (JCE).[28] A JCE is a separate proposal from the BCS and would create a common environment for federal agencies to quickly share and analyze data from across the federal government (regardless of classification) and from the private sector. If both the proposed JCE and BCS are implemented, then it is likely that the BCS would collect data directly from sources and provide information products that the JCE would use in conjunction with other information sources to inform government operations related to cybersecurity.

CISA Data Sources and Limitations

Arguably, CISA is the agency that has the most comprehensive access to data on cybersecurity incidents in the federal government. Because of this, CISA is frequently discussed as the home of a potential BCS. Despite the agency's current information, it likely does not have access under its existing authorities to all the information necessary for a federal statistical agency.

CISA gathers information from three sources: (1) direct collection; (2) information sharing; and (3) acquisitions. The data in CISA's possession suffer from the same drawbacks as discussed above: the data are (i) not uniform, (ii) incomplete, and (iii) housed in datasets, which are not scrubbed, ready, or prepared for combined use.

CISA operates a variety of programs to collect cyber risk information directly. The agency collects information from sensors deployed on federal agency networks, such as the National Cybersecurity Protection System (NCPS),[29] an integrated system for intrusion detection and

[26] Department of Homeland Security/Office of the Inspector General, *DHS Made Limited Progress to Improve Information Sharing Under the Cybersecurity Act in Calendar Years 2017 and 2018*, OIG-20-74, September 25, 2020, at https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf.

[27] U.S. Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288, March 2021, pp. 61-63, at https://www.gao.gov/assets/gao-21-288.pdf.

[28] Sara Friedman, "Rep. Langevin Plans to Push for Joint Collaborative Environment Legislation to Accelerate JCDC Efforts," *Inside Cybersecurity*, March 31, 2022, at https://insidecybersecurity.com/daily-news/rep-langevin-plans-push-joint-collaborative-environment-legislation-accelerate-jcdc.

[29] Cybersecurity & Infrastructure Security Agency, "National Cybersecurity Protection System," website, at https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

prevention, and the asset and vulnerability inventorying Continuous Diagnostics and Mitigation program (CDM).[30] Per law[31] and OMB direction,[32] agencies are required to report to CISA when they experience cybersecurity incidents. Additionally, CISA accepts voluntary cyber incident reports from the public and private sectors.[33]

CISA receives information from both public and private entities related to cyber incidents. Sector risk management agencies have agreements with CISA to share cybersecurity risk information. For example, the Food and Drug Administration signed a Memorandum of Agreement with the precursor agency to CISA (i.e., the National Protection and Programs Directorate) related to medical device cybersecurity.[34] Private entities also share information with CISA. For example, prior to making their public release on the SolarWinds vulnerability and its exploitation by Russia, the cybersecurity firm FireEye notified CISA of the ongoing investigation, which gave the agency a head start on developing response guidance.[35] CISA may collect freely available data sets, such as those published by researchers.[36]

CISA may also acquire threat intelligence from a cybersecurity firm, just the same as any private sector entity may purchase or subscribe to such services. For example, CISA has a subscription to Mandiant Threat Intelligence.[37] However, as with other sources of information, data from these feeds may not be easily combined with other data sources to be analyzed by automated means, may not contain information relevant to the government's analytic purposes, or may carry restrictions on how the data may be used.

Additionally, data not directly collected by the agency are aggregated by the original collector to protect privacy. This forces secondary analysis as opposed to primary review of data. Such analysis may still prove valuable, but does not provide the same level of granularity and precision, as it relies on data collected (including the collection methodology) and analyzed by another party, rather than tailoring the data collection, analysis, and publication to the agency's statutory purpose.

[30] Cybersecurity and Infrastructure Security Agency, "Continuous Diagnostics and Mitigation (CDM)," website, at https://www.cisa.gov/cdm.

[31] 44 U.S.C. §3554.

[32] Office of Management and Budget, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, M-22-05, December 6, 2021, at https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf.

[33] "Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government," fact sheet, at https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf.

[34] "Memorandum of Agreement Between the Department of Homeland Security, National Protection and Programs Directorate and the Department of Health and Human Services, Food and Drug Administration, Relating to Medical Device Cybersecurity Collaboration," MOU 225-19-002, April 9, 2019, at https://www.fda.gov/about-fda/domestic-mous/mou-225-19-002.

[35] See CRS Insight IN11559, *SolarWinds Attack—No Easy Fix*, by Chris Jaikaran.

[36] For an example, see Verizon, "Data Breach Investigations Report," report, 2022, at https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf.

[37] Mandiant, "DHS Shared Cybersecurity Services," data sheet, 2021, at https://www.fireeye.de/content/dam/fireeye-www/products/pdfs/pf/gov/dhs-intelligence-subscription.pdf.

Considerations for CISA Undertaking BCS Responsibilities

The Commission identified five distinct attributes for a BCS: (1) definition of cybersecurity metrics; (2) collection and aggregation of cyberattack data; (3) reporting mandates for incidents; (4) data and privacy protection; and (5) information exchange between academia and the private sector. Each attribute is discussed further below with implications for CISA. An additional attribute of analytic capabilities is also discussed.

Defining Cybersecurity Metrics

This attribute relates to the authorization in the model legislative text for the proposed BCS to collaborate with NIST on measures and metrics. As discussed above, much cybersecurity risk data exists among federal and nonfederal entities today. However, the data object values that are pertinent to national policymaking and private sector decisionmaking have not been articulated. Industry has expressed reservations about government collection of information related to cybersecurity matters as the very information technology (IT) systems that experience the incidents may also hold sensitive data that victims may not want exposed to third parties, including the government.[38] This concern may be raised again as a BCS capability seeks to define the metrics necessary to perform statistical analyses. Additionally, statistical models for analyzing cybersecurity datasets have not been developed. If the government were going to require entities to report cybersecurity data to a new federal statistical agency, then national stakeholders would likely expect such an agency to adhere to the principles of federal statistical agencies—particularly developing credibility among data users and trust among the data providers. Transparent metrics and analytical methodologies are generally accepted practices for achieving those goals.

As an agency, CISA has not yet had to delve into statistical agency activities, so establishing a BCS would require new lines of effort. Explicit congressional authorization for CISA to perform these duties (particularly data collection) would help the agency build relationships with the organizations that would be required to share information. NIST and CISA have a history of working together and may be likely partners in developing such a capability. During the Obama Administration, the agencies partnered in developing and disseminating the *Framework for Improving Critical Infrastructure Cybersecurity*[39] and recently the agencies released a joint statement on performance goals developed for critical infrastructure industrial control systems pursuant to a National Security Memorandum.[40] While NIST could assist CISA in developing CISA's statistical capability, other federal entities may also be able to provide support. The National Science Foundation-funded Committee on National Statistics, as well as other statistical agencies (e.g., BLS), may be able to provide expertise, experience, and education in support of building out a statistical capability for the proposed BCS.

[38] U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, 117th Cong., 1st sess., September 1, 2021, Serial No. 117-28 (Washington: GPO, 2021).

[39] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Framework," website, at https://www.cisa.gov/uscert/resources/cybersecurity-framework.

[40] Department of Homeland Security, "Joint Statement by Secretaries Mayorkas and Raimondo on President Biden's National Security Memorandum to Strengthen Nation's Cybersecurity Infrastructure," press release, September 22, 2021, at https://www.dhs.gov/news/2021/09/22/joint-statement-secretaries-mayorkas-and-raimondo-president-biden-s-national.

Collecting and Aggregating Data

This capability refers to the BCS's ability to acquire necessary data and conduct pertinent analysis. The model legislative text discusses options for the BCS administrator to enter into agreements with other federal agencies to share existing data. The proposed BCS may also create mandates for industry and agencies to directly report on data object values. The proposed BCS may need to purchase data from private sources, and the Commission advocates for a BCS to be resourced sufficiently to make those purchases regularly.

As discussed above, CISA currently has some experience in entering into agreements with other federal agencies for cybersecurity information sharing and has subscribed to services providing threat intelligence. CISA's fiscal year 2023 congressional budget request asks for increases to current programs related to purchasing privately held data for federal analysis—particularly to support information and communications technology supply chain risk assessment and to provide cyber threat intelligence feeds to other agencies as part of a shared service.[41] It is likely that CISA would require an increase in resources in order to acquire (through either agreement or purchase) and manage the data necessary to carry out BCS responsibilities.

Reporting Mandates for Incidents

This attribute relates to the requirement for entities (private and public) to report information to BCS in order to inform statistical analysis.

Congress has already legislated a requirement to report incidents. Division Y of the Consolidated Appropriations Act, 2022 (P.L. 117-103)—named the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[42]—requires CISA to (1) engage in rulemaking to mandate private sector reporting of cybersecurity incidents to the agency; (2) enforce noncompliance with required reporting; and (3) disseminate analysis based on the information collected. CISA is currently working with stakeholders on developing the notice of proposed rulemaking.

Protecting Data and Privacy

This attribute relates to the potential confidentiality of data provided and the requisite protections those data may require. As a federal agency, CISA is already subject to the data protection provisions pursuant to the Federal Information Security Modernization Act (P.L. 113-283)[43] and the privacy protections of individuals under the Privacy Act (P.L. 93-579).[44] As a statistical agency, CISA would be subject to further requirements under CIPSEA and OMB's regulations and directives for the federal statistical system.[45]

CIRCIA extends data protections found in the Cybersecurity Act of 2015 (P.L. 114-113, Division N) to data collected for the cyber incident reporting and creates explicit limitations for the purposes of data collected, the sharing of that data, and requirements to protect that data. Here

[41] Department of Homeland Security, *Cybersecurity and Infrastructure Security Agency Budget Overview*, Fiscal Year 2023 Congressional Justification, March 2022, pp. O&S 30-31, https://www.dhs.gov/sites/default/files/2022-03/Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29_Remediated.pdf.

[42] 6 U.S.C. §§681a-g.

[43] 44 U.S.C. §§3551-3559.

[44] 5 U.S.C. §552a. For more information see, CRS Report R47058, *Access to Government Information: An Overview*, by Meghan M. Stuessy.

[45] 44 U.S.C. §§3561-3564.

again, CIRCIA's requirements for CISA may be extended to the BCS capability should Congress choose to assign such activities to CISA.

Exchanging Information Between Academia and the Private Sector

This attribute relates to the recognition that federal statistical agencies engage in academic research and should strive to share methods, techniques, and analysis with the research community, contribute to innovations, and provide forums by which public and private sector entities can engage. CISA has a history of engaging the cybersecurity research community in the discovery and disclosure of novel technological vulnerabilities and has been host to many public-private fora on critical infrastructure security and resilience and cyber risk management. However, those activities were generally in support of CISA's programs and not in furtherance of national data on cybersecurity, which may require different engagement strategies.

A BCS would be expected to expand the body of knowledge and advance research opportunities for cybersecurity risk data. These would be new outcomes for CISA, but the programmatic considerations of such activities are already familiar to the agency. Should Congress choose to assign BCS activities to CISA, the agency may benefit from explicit authorization related to such engagements—both to require the agency to regularly conduct them and to encourage researcher participation in the exchange.

Analyzing Data

The Commission did not explicitly discuss the *analytic capability* necessary for a BCS to develop analytic products, although it was considered as part of the first two attributes. Following the principles of federal statistical agencies, developing transparent methodologies so that stakeholders may have confidence in the published products would be critical to the proposed BCS's success. Here again, CISA would likely need assistance from NIST and existing statistical agencies in developing these models. However, CISA may be able to leverage existing partnerships in order to acquire and use technical capabilities to perform and interpret analyses. CISA's National Infrastructure Simulation and Analysis Center (NISAC, an element of the National Risk Management Center)[46] works with the National Laboratories[47] and Federally Funded Research and Development Centers (FFRDCs)[48] to acquire data and perform analyses to inform models related to projecting the cascading effects of information technology failures among critical infrastructure industries. These capabilities may be useful to a BCS capability, but would likely be supplemental.

[46] Cybersecurity and Infrastructure Security Agency, "National Infrastructure Simulation and Analysis Center," website, at https://www.cisa.gov/NISAC.

[47] Department of Energy, "National Laboratories," website, at https://www.energy.gov/national-laboratories.

[48] National Science Foundation, "Master Government List of Federally Funded R&D Centers," website, February 2022, at https://www.nsf.gov/statistics/ffrdclist/.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer