DRAFT REPORT TO THE CISA DIRECTOR

Corporate Cyber Responsibility

September 13, 2023

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Corporate Cyber Responsibility (CCR) subcommittee to research ways to encourage a nationwide culture of corporate responsibility where cyber safety is incorporated into all executive decisions and how to encourage, enable and support private sector boards and C-Suite executives to reduce cyber risk as a matter of good governance. Cyberattacks and their impact could be better mitigated or even prevented if corporate boards of directors were more educated and engaged on matters relating to cybersecurity, placed a higher priority on cyber resilience, and exercised stronger oversight over the development and execution of their companies' cybersecurity strategies.

CISA provided an initial set of six framing questions to guide the work. These questions are below, with corresponding notations as to where each question is addressed within this report:

1. How should CISA work with board members and shareholders of public companies to encourage them to take a more active role in cybersecurity?
   This question is addressed throughout the report within multiple recommendations.

2. How can CISA help board members and shareholders understand the impacts of companies' cyber risk management practices and advocate for the adoption of cybersecurity best practices?
   This question is addressed throughout the report within multiple recommendations.

3. How can CISA best structure its guidance and outreach so it reaches board and C-Suite audiences? How should this outreach differ, if at all, for public and non-public companies?
   This question is addressed throughout the report within multiple recommendations.

4. How can CISA measure the effectiveness of the CCR effort?
   See recommendation within Pillar IV/Sustained Leadership and Collaboration concerning the designation of a high-level CISA official with industry experience who should have responsibility for overseeing and measuring the effectiveness of CISA's CCR effort.

5. What lessons can CISA draw from movements that have sought to use shareholder or board influence to change company practices, for example, on environmental or social issues?
   See recommendation within Pillar I/Board Member Education intended to bring cyber resilience to the forefront of investor decision-making.

6. Should CISA encourage credit rating companies to establish ratings of companies' cyber risk? If so, what should they measure? What are the possible downsides of introducing such rating systems?
   See recommendation within Pillar II/Measurement concerning the use of tools developed by credit ratings companies that may assess cyber resilience, readiness, or compliance.

The recommendations were informed by a series of briefings involving participants from corporate governance and corporate cybersecurity governance communities. It divided its work into three main phases:

1. Evaluating the lines of effort (LOEs) that CISA currently has to draw more attention to the specific actionable steps board members and C-Suite corporate officials can take to better secure their companies (including working with national organizations representing these stakeholders);
2. Exploring drivers and potential drivers of director behavior to understand how best to motivate them to take a more active role on cybersecurity matters; and
3. Developing actionable recommendations to CISA for how to encourage the behavior it seeks from corporate boards relating to how to ensure directors and management understand that cyber risk is one of several business and operational risks and that managing it is critical to a company's financial health.

Findings

High-profile breaches, especially those that have occurred over the past few years, have impacted a wide array of public corporations, and drawn national attention to the risk that cyberattacks pose, not just to business continuity and profitability but to the continuity of our society. Ransomware is having devastating effects on U.S.-based companies and organizations and the citizens that rely on services provided by them, especially those in critical sectors. The current cyber threat against American corporations and by extension the U.S. economy is of the same level of magnitude and seriousness as the conditions that led to the 2001 world financial crisis. Corporate financial scandals involving Enron, WorldCom, and other companies ushered in a new era of accountability for public company directors. The impact of the crisis was so profound that the government, among its many responses, created more robust standards for corporate oversight and accountability. These standards included new rules concerning board independence, the implementation and strengthening of internal control systems, and restrictions on the provision of non-audit services by external auditors, just to name a few. Over the past three years, U.S. corporations have faced cyberattacks that pose an extreme level of risk. It is estimated that by the year 2025, cybercrime will cost the world $10.5 trillion annually.[1] IBM has estimated that the average cost of a data breach globally is $4.45 million.[2] Recent notorious attacks have included the SolarWinds, Colonial Pipeline, Log4j and, more recently, the MOVEit breaches, as well as the insidious ransomware epidemic that seems to disproportionately affect vulnerable critical sectors (e.g. education and healthcare) and small businesses. This dire trend necessitates that the U.S. government and CISA take serious action to stem the crisis and curb future risks from threatening the continuity of our sectors, economy, and society. Increased corporate responsibility must lie at the center of these actions, much as it did in the wake of the world financial crisis.

The members of the Subcommittee have significant combined experience serving on, communicating with, and supporting corporate boards. Individuals in this group have struggled with or witnessed first-hand the barriers to effective board governance of cybersecurity and are pleased to offer their recommendations to the CISA Director. The recommendations generally can be categorized into four main areas (Pillars): **Board Member Education, Measurement, Responsibility and Sustained Leadership, and Collaboration**.

I. **Board Member Education**: The U.S. must find a way to eliminate the "cyber literacy chasm." There is a major gap in the knowledge directors have of cybersecurity issues broadly and about the components of strong cybersecurity programs. There will never be enough Chief Information Security Officers (CISOs) to staff every board, and it is imperative that board members develop more cyber literacy and competency. Not every board member needs to be an expert in understanding and addressing the cybersecurity concerns of the company, but more board members need to be far better educated on how to understand cyber risk, how to better listen to and understand CISOs, and how to better evaluate the effectiveness of their companies' cybersecurity plans. All board members should have a basic level of education on cybersecurity issues. Education also means CISOs should be enabled to become more effective listeners and communicators with, and to, directors. More education on both sides will enable a more effective and sustained relationship between directors and CISOs. Efforts to educate board members about cybersecurity are not new: leading stakeholders including the National Association of Corporate Directors (NACD), Diligent Corporation, the Institute for Shareholder Services (ISS), and NASDAQ have created some highly effective approaches. Efforts to make CISOs more adept at communicating

[1] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[2] https://www.csoonline.com/article/567697/what-is-the-cost-of-a-data-breach-3.html

with boards are also not new, and here we point to the work of Digital Directors Network (DDN), ISC2 and others. While very effective, these efforts have not necessarily been able to scale to the extent that is needed to account for the multitude of U.S. corporate boards in need of this transformation.

II. **Measurement**: There needs to be improved data and metrics concerning the level of cyber literacy and competency of directors. Additionally, there must be more availability and uniformity of data concerning cyber risk within enterprises to enable both CISOs and directors to perform their duties. Directors must have access to relevant and timely information, avoiding excessive filtering through management layers, and be able to use that information to assess cyber risk and performance and, with firm management, implement changes.

III. **Responsibility**: There must be clearer lines of responsibility and accountability drawn between stakeholders responsible for ensuring the cyber resilience of corporations. This conversation has been accelerated by the Securities and Exchange Commission's (SEC) proposed cybersecurity rules that would require publicly traded companies to disclose a cyber incident within four business days upon determination of materiality and to provide disclosure in periodic reports about certain cybersecurity governance practices. While CISA does not have jurisdiction over requirements for corporate boards, it can play an important role in shaping the conversation about what is expected of companies and their directors. This Pillar will discuss how to encourage board members to take a more active role in cybersecurity, will recommend the creation of best practices for board governance and then suggest ways to ensure corporations are following these best practices. This Pillar will also suggest ways to ensure boards and corporations follow cybersecurity best practices including through new or amended requirements relating to the implementation of known cybersecurity risk management frameworks and the creation of principles and accompanying best practices for cyber-responsible boards. It will also discuss the question of board structure.

IV. **Sustained Leadership and Collaboration**: Directors are becoming more involved in matters of cybersecurity governance as the risks and impacts associated with cyberattacks have an outsized impact on company performance, reputation, and liability. While cybersecurity issues are much more broadly discussed and understood today, CISA, in partnerships with other stakeholders, can do more to incentivize directors to be more engaged and give them the tools exercise more diligent and informed oversight. CISA has been providing crucial leadership on corporate cybersecurity governance by creating various guidance documents and collaborating with stakeholders to address specific needs. CISA released the Cybersecurity Performance Goals (CPGs), which establish a common set of fundamental cybersecurity practices for critical infrastructure with known risk-reduction value.[3] CISA continues to work with both Sector Risk Management Agencies (SRMAs) and industry to develop Cross-Sector Cybersecurity Performance Goals that will address safety practices that may be unique to a given sector, as well as sector-specific approaches to implementing the cross-sector goals.[4] CISA also worked with the NACD in the development of an updated Director's Handbook on Cyber-Risk Oversight and to create the Certificate in Cyber-Risk Oversight Program[5] for mature boards ready to take an additional step in cybersecurity oversight. This Pillar will recommend ways CISA can strengthen the cooperation amongst all stakeholders in this ecosystem and leverage and build upon work that is already underway. Implementing the recommendations in this report will require CISA to dedicate more personnel to corporate cyber responsibility, including a designated senior staff leader with several direct reports, to coordinate and oversee CISA's ongoing CCR efforts and to ensure it has sustained and structured partnerships that allow it to team with the right stakeholders to accomplish these objectives.

With respect to time horizon, several of the Subcommittee's recommendations warrant immediate attention. The Subcommittee designates such recommendations by stating that they should be implemented "as soon as practicable." Five of the recommendations included in this report fall into this category: Obtaining the necessary data about the gap in director education about cybersecurity (Pillar I/Board Member Education/1); Expanding and enhancing educational

[3] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[4] https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf
[5] https://www.nacdonline.org/events/detail.cfm?ItemNumber=37092

offerings and training for directors (Pillar I/ Board Member Education/4); Obtaining the necessary data to assess how well directors provide oversight to firms on cybersecurity matters (Pillar II/Measurement/1); Developing Performance Goals for Cyber-Responsible Boards that advances a set of principles and best practices for cyber-responsible boards (Pillar III/Responsibility/5); and Designating a high-level official to lead a line of effort around increasing national corporate cyber responsibility (Pillar IV/Sustained Leadership and Collaboration/1).

The Subcommittee agreed that it was crucial to first identify the potential and actual drivers of director behavior to inform its recommendations. These drivers are key to motivating directors to become better educated, engaged, and accountable on matters of cybersecurity. After considerable discussion internally and with subject matter experts, the Subcommittee summarizes these drivers as follows:

1. **Regulations:** That directors' behavior is directly and strongly influenced by regulations, both federal and state, needs little explanation. Regulations can pertain to high-level governance issues, or they can contain mandates to implement specific security controls. An example of the former includes the SEC's proposed Cybersecurity Risk Governance Rule for Public Companies, which contains mandates around governance issues such as required disclosure of cybersecurity policies and procedures and providing adequate information to shareholders.[6] Examples of the latter include the Transportation Security Administration's (TSA's) Security Directive for Pipelines or the New York Department of Financial Services' 23 New York Codes Rules and Regulations (NYCRR) Part 500.[7,8]

2. **Audits:** Auditors conduct assessments of how well companies have met the aforementioned regulations. These assessments generate findings, which in turn require management, with the approval of directors, to take specific corrective actions. The requirement that a company reports material weaknesses or significant deficiencies relating to cybersecurity will, over time, alter director behavior more than any other single driver, as evidenced by the effectiveness of controls required of companies by the Sarbanes-Oxley Act of 2002. This is addressed in Pillar II/Measurement (Measuring enterprise cyber risk) and Pillar III/Responsibility (Create common controls, measurement, and reporting).

3. **Civil and criminal liability**: Class action lawsuits send a strong signal to directors and management that there exists a duty of care to stakeholders that must be followed. The case of one Uber executive being found criminally liable for not disclosing a breach of consumer data serves as a powerful example.[9]

4. **Risk transfer markets:** The availability and cost to companies of insurance policies that cover the effects of financial risk resulting from cyberattacks impact board behavior. In underwriting cybersecurity insurance policies, insurance companies have an extensive list of questions companies must answer. If companies do not maintain strong cybersecurity programs, including following known frameworks, then insurance policies will be much more expensive or even unavailable.

5. **Brand risk**: When a breach or cyber incident becomes public, companies can suffer a degradation of their brand, which in turn diminishes shareholder value. Board members will therefore endeavor to reduce brand risk owing to cyberattack by diligently overseeing cybersecurity programs.

6. **Duty of care:** Cybersecurity regulations commonly directed by specific U.S. federal agencies at companies within critical sectors under their purview are usually derived from National Institute of Standards and Technology (NIST) Special Publication 800-53. Yet not all publicly traded companies are considered to fall within "critical

[6] https://www.sec.gov/news/press-release/2023-52-
[7] https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf; https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
[8] https://www.dfs.ny.gov/industry_guidance/cybersecurity
[9] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data

sectors" and are therefore not required to implement a specific set of controls such as these frameworks prescribe. Many companies adopt NIST 800-53 or the NIST Cybersecurity Framework (CSF), or another cybersecurity risk framework such as the Center for Internet Security (CIS) Controls, MITRE ATT&CK framework, or the CPGs. But for many companies, following such a cybersecurity risk management framework is not required. Companies should, however, adopt one of these frameworks because they are increasingly providing the elements for the duty of care (i.e. minimum expected actions) for corporations to ensure cyber resilience. Especially when combined with some of the aforementioned drivers (e.g. civil liability), these frameworks as well as any additional future cybersecurity requirements placed upon companies have a powerful influence on director behavior.

7. **Investor Awareness:** Directors have become increasingly more educated and aware of environmental, social, and governance (ESG) issues because institutional investors and pension funds are considering the environmental and social impact of their portfolios to a far greater to degree. We must strive to ensure investors are educated about the impact of cybersecurity risk within their portfolios.

Recommendations

Pillar I/Board Member Education

This Pillar addresses the most critical education gap, which is the need to create stronger cybersecurity knowledge and expertise among board members.

- Produce a report on the board director education gap. As soon as practicable, CISA should initiate a collaboration with relevant stakeholders to produce a data-driven report that enumerates the cyber literacy gap in the boardroom.
  - Relevant and accurate data is needed on the cybersecurity literacy of directors on U.S. corporate boards to understand the scope and impact of the problem as well as to define the knowledge gap that exists between board members and CISOs. CISA should conduct an assessment on the "state of cyber literacy in the boardroom" that measures and describes the cyber literacy gap that exists between directors and CISOs. A section of this report should be devoted to assessing the literacy gap of directors of non-public companies.
- Establish expected levels of cybersecurity knowledge for board directors. CISA, in coordination with other stakeholders, should create and promote an expectation of the baseline level of knowledge about cybersecurity all directors should have and should create recommendations for a standardized cybersecurity curriculum for directors to be incorporated into training offerings.
- CISA, in coordination with other stakeholders, should determine levels of cybersecurity proficiency for directors above the baseline level of knowledge referenced above.
- Expand and enhance training. As soon as practicable, CISA should work with relevant stakeholders to expand and tailor existing educational offerings for directors to ensure all directors have the recommended baseline level and to help more directors attain higher levels of cybersecurity proficiency.
  - In doing so, CISA should partner with other federal agencies to leverage existing methodologies, programming, and content.
  - For example, CISA could partner with the U.S. Secret Service, which runs a training program for directors at their training facility, the J.J. Rowley Training Center in Beltsville, Maryland. CISA should work with board management software providers to build cybersecurity training/learning/evaluation modules into their platforms.
  - For example, CISA could lead the development of three- to five-minute educational videos and quizzes that are presented within their board software management platforms. Training and educational materials could be delivered as additive, optional offerings within these platforms or could be required, in order for directors to access their board materials. CISA should adapt these offerings for use by non-public company board directors.

- Deliver training at scale. CISA, in coordination with other stakeholders, should encourage and help lead the creation of a centralized cyber education platform, including creating content into which all stakeholders can integrate. This will provide stakeholders with a continuous method for enhancing their cyber literacy.
  - Training opportunities should be delivered at scale and continuously, not just in once-a-quarter or once-a-year posture, and not just when directors access their board materials.
  - Once established, CISA should actively promote educational and training resources and opportunities for board members and CISOs so that these resources are widely known and utilized.
- Promote director certification and accreditation. CISA should encourage the broader adoption of cybersecurity certifications and accreditations like what is offered today by NACD, ISC2 and other stakeholders. NACD's certification includes cybersecurity content aligned with business resilience exposures.
- CISA should use its influence and voice to encourage companies to look for this certification in selecting directors and to weigh the attainment of this certification in their director selections.
- Educate about business imperative. CISA should work with partners to develop quantitative and qualitative analyses demonstrating the relationship between inadequate cybersecurity programs and business and operational risk and by actively and broadly discussing and promoting this concept among all stakeholders.
  - The key to educating and motivating directors lies in demonstrating to directors and management that cyber resilience is a business imperative.
- Expand and enhance training for other stakeholders.
  - More education and training are needed for other stakeholders, especially CISOs, so they can better communicate with directors. Resources are also needed to better educate other stakeholders, including regulators, auditors, insurers, and investors. The training platform described above could be adapted to support the education and training of other types of stakeholders. CISA should study the question and incorporate its findings into future LOEs.
- CISA should work with other relevant federal agencies and stakeholders to generate Principles for Cyber-resilient Investing, the purpose of which shall be to bring cyber resilience to the forefront of investor decision-making. These principles could be modeled after the Principles for Responsible Investment developed in 2006 by an organization affiliated with the United Nations, the purpose of which was to promote the incorporation of environmental, social, and corporate governance factors (ESG) into investment decision-making.[10]

Pillar II: Measurement

The Committee lacks the right data, and even the right methods for collecting such data, to assess how well directors provide oversight to firms on cybersecurity matters. More relevant and accurate data, new data collection methodologies and guidance on recommended best practices are needed in a few key areas. These areas include: 1) Director cyber knowledge, engagement, and effectiveness; 2) Effectiveness of communications between directors and management on cybersecurity matters; 3) Effectiveness of board oversight; and 4) Enterprise cyber risk.

- Identify data deficiencies. CISA should work with other stakeholders to identify areas where data is deficient and to seek new data sources for these.
  - As soon as practicable, CISA should identify areas in which more relevant and accurate data is needed. These areas include, but are not limited to:
    - Director education, engagement, and effectiveness,
    - Effectiveness of communications between directors and management on cybersecurity matters,
    - Effectiveness of board oversight, and
    - Enterprise cyber risk.
- Measure director engagement. CISA, in collaboration with relevant U.S. agencies, should develop a list of research and data that is necessary to assess directors' level of education and engagement on matters of cybersecurity oversight.

[10] https://www.unpri.org/about-us/about-the-pri

- CISA, in partnership with relevant agencies and stakeholders, should promulgate guidance on how to measure director engagement and director effectiveness in executing their responsibilities.
- Measure the effectiveness of communications. CISA should determine what data and metrics are needed in this area, and then develop guidance on best practices in communications between management and boards, including what level of technical detail and preferred formats and modes for transmission of such information.
- CISA should develop a subset of this guidance as it pertains to directors of non-public companies.
    - Directors must have access to relevant and timely information from management and must be able to use that information to assess cyber risk and performance and, with firm management, implement changes. CISA can weigh in on methods, including platform-based technologies, which some companies find significantly facilitate communications.
- Measure the effectiveness of board oversight. CISA, in partnership with relevant stakeholders, should develop a Framework for Effective Board Oversight.
    - The Framework for Effective Board Oversight (Framework) should describe best practices in board governance and could include recommendations on "governance controls," including how often a board should be briefed by a CISO, how it should structure itself with respect to committees, how it should best utilize insurance products and third-party assessments tools.
    - The Framework should include resources such as exemplary committee charters, lists of common risk factors, approaches for enterprise risk management (ERM), and resolving critical audit matters (CAMs). The Framework could also enumerate and clarify the types of business and financial factors that should be contemplated when determining incident materiality.
    - The Framework should contain methodologies for measuring boards' progress in implementing the Framework, meeting the stated goals stated of its cybersecurity plans, addressing findings and MWs, and increasing the firm's overall operational resilience.
    - In creating the Framework, CISA should draw upon existing work from NACD, DDN, World Economic Forum, and NIST.[11] Eventually, a variant of this Framework should be created for directors of non-public companies.
- Measure enterprise cyber risk.
    - Several proven cybersecurity risk management frameworks exist, but companies are confused and need guidance on which one they should adopt and how to implement it. At the direction of the President, the Office of the National Cybersecurity Director, Office of Management and Budget and Independent and Executive Branch Regulators are in the process of harmonizing baseline cybersecurity requirements for all companies deemed to be part of a critical sector. However, the July 2021 National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems directed CISA and NIST to develop the CPGs, referenced above, and these should serve as the prevailing cybersecurity risk framework all companies should use, especially when no other set of cybersecurity controls is mandated by regulation.
- CISA, in partnership with the White House and SEC, should consider whether corporations should be required to adopt CPGs as the cybersecurity risk management framework against which they must report. This requirement could apply to all publicly traded companies or could apply only to those that are not already required by a U.S.-based regulatory agency to implement a NIST-based set of cybersecurity controls.
- CISA, in partnership with public and private sector stakeholders, should hold a series of workshops demonstrating how companies effectively implement the CPGs or other cybersecurity risk management frameworks.
    - These workshops should showcase examples of how firms measure their progress in implementing such frameworks and how well the implementation of these frameworks contributes to firms' overall cyber resiliency and cybersecurity risk reduction. These workshops should showcase approaches and technologies that allow management and boards to understand the correlation between the implementation of cybersecurity risk frameworks and specific controls to reduce cyber risk.
- Manage risk transfer. CISA should study the criteria used by underwriters in setting cybersecurity insurance

[11] The NIST Cybersecurity Framework 2.0, released on August 8, 2023, contains a new function, "Govern," to cover organizational context; risk management strategy; cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and oversight. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

policies and establish practices for managing risk via the risk transfer markets to understand the role of risk transfer more accurately in influencing corporate and director behavior and to inform the promulgation of guidance recommended elsewhere in this report.
    - The financial risk resulting from cyberattacks can be managed to some extent by transferring risk via insurance policies. Insurance companies assess firms' cybersecurity risk readily and well.
- Utilize third party assessments. CISA should promulgate guidance that includes best practices and recommendations for how companies can successfully incorporate such capabilities into their cyber risk assessments.
    - Many firms utilize third-party security ratings tools which provide an "outside-in" assessment of how firms are meeting common cybersecurity benchmarks. Directors have increasingly become aware of and may leverage such tools.
- Stay neutral on cyber risk ratings by credit rating agencies. CISA should not encourage credit rating companies to establish ratings of companies' cyber risk.
    - If credit ratings companies develop products aimed at assessing cyber resilience, readiness, or compliance they can provide useful data to directors and managers, but they do not constitute a definitive means of assessing a firm's cyber risk. In June of 2023, the SEC directed all federal agencies to reduce reliance on and references to credit ratings in agency regulations.[12]

Pillar III/Responsibility

We must draw lines of responsibility and accountability for and between stakeholders in key corporate roles, define what is needed to ensure directors are responsible and accountable, and foster stronger and more effective communication and coordination amongst stakeholders.

- Help directors build better understanding of business impact. CISA should create materials that explain the loss and liability to companies for certain types of cybersecurity events.
    - The greatest single factor that will generate more director engagement is to create commonly accepted ways of quantifying and demonstrating the business impact of firms' failure to implement an effective cybersecurity strategy, including adopting a known cybersecurity risk framework. It can do so quantitatively through financial modeling, and it can do so qualitatively by emphasizing the stories and experiences of other companies.
- CISA should create methods for directly linking certain actions and non-actions, as well as investments and failure to invest, to potential cyber risk and then, in turn, communicate that risk in dollar amounts.
- CISA should conduct and publish research on this question and in doing so, should ask the industry to collaborate and provide data.
    - If the cybersecurity risk management frameworks like CPGs, NIST CSF, MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and CIS Top 20 represent the most important controls for companies to implement, then directors must understand how much they reduce their risk by implementing them and how much they increase their risk by not implementing them.
- Generate more relevant and accurate data. CISA should create such a data set and continually update it, with assistance from the Information Sharing and Analysis Centers (ISACs) and the insurance industry.
    - Relating directly to the above and to Pillar III/Measurement, more relevant and accurate data is needed for companies to be able to quantify the business impact of cyber risk. Companies not only need more comprehensive insights into risk across their enterprises preferably in real or near-real time (some companies use network monitoring tools that may provide this, some do not), but they also need sector-wide actuarial data that helps them understand their own risk in the context of their corporate profile.

[12] https://www.sec.gov/news/statement/lizarraga-statement-credit-ratings-060723

- Create Performance Goals for Cyber-Responsible Boards. CISA, in collaboration with relevant stakeholders, should create Performance Goals that contain a set of principles and accompanying best practices for cyber-responsible boards to help directors focus their efforts and attention and help their firms improve cybersecurity outcomes.
    - These Performance Goals should enable directors to view cybersecurity from a position of empowerment rather than fear. CISA should begin this work as soon as practicable, given a reasonable timeline for obtaining the data needed to inform the effort. The Performance Goals should:
        - Define what is an adequate level of training and knowledge for board members on cybersecurity oversight, noting that all members of the board should have some baseline knowledge of and be engaged in cybersecurity matters, not just those serving on relevant committees (overlaps with Pillar I/Board Member Education).
        - Describe board members' core responsibilities pertaining to cybersecurity which, among other things, include approving cybersecurity policies, overseeing cyber risk management, and verifying regulatory compliance.
        - Illustrate examples of well-drawn lines of responsibility and accountability between stakeholders in these roles.
        - Provide examples of how boards can achieve effective communication and coordination among stakeholders.
    - Illustrate variants of board structures that work well for companies, including how management reports to the board and board committees. CCR does not endorse the creation of a cybersecurity committee because it lacks business, operational and financial context which introduces a disconnect between the management team and the broader board membership. CCR does support cybersecurity oversight residing in the risk committee that contains complementary risk domains such as privacy, supply chain and geopolitical. CISA should allow flexibility in its guidance on board structure, especially in recommending what works well for companies of certain sizes and types.
    - Illustrate variants of committee charters that work well for different companies. CISA should partner with relevant federal agencies and other stakeholders to publish an exemplary charter of the committee responsible for cybersecurity oversight, make it a public document and make it flexible enough for different types of companies dealing with different (and changing) regulatory requirements and controls.
    - CISA should create a parallel set of principles and accompanying practices aimed at board directors for non-public companies.
- Create common controls, measurements, and reporting. Consistent with the recommendations included in Pillar II/(Measure enterprise cyber risk), CISA should work with the White House and the SEC to consider whether the CPGs should serve as the prevailing baseline of controls against which determinations of material weaknesses (MWs) and significant deficiencies (SDs) are made for the purposes of SEC reporting, whether for all companies or only for those that are not already required by a U.S.-based regulatory agency to implement a NIST-based set of cybersecurity controls.
    - New SEC cybersecurity rules adopted in July 2023 would require publicly traded companies to disclose a cyber incident within four business days and to provide disclosure in periodic reports about certain cybersecurity governance practices. However, the rules do not include requirements concerning what companies should be doing to increase their cyber preparedness and resilience. Having a common set of cybersecurity controls that all public companies must implement will make it clear what companies must do, as well as create a common set of measurement and reporting methodologies that assess and communicate companies' implementation of the required controls. How determinations of MWs and SDs are made represents the single greatest factor influencing director behavior and therefore firms' overall cyber preparedness and resilience. Directors act to immediately address such findings when they appear, including by making resources available to CISOs.
- Amend CPGs to include flow-down to suppliers and encouragement of secure-by-design. CISA should adapt the CPGs to include, under "Vendor/Supplier Cybersecurity Requirements," questions to suppliers and potential suppliers regarding their board governance practices (to determine how much oversight their boards provide and

how engaged they are on cybersecurity matters) as well as questions about their implementation of a widely accepted cybersecurity risk management framework.
    - Ensuring that the products sold do not cause people harm is a board-level responsibility, demonstrated over many decades and across many industries. Companies that produce hardware and software are not exempted from this responsibility with regard to weaknesses and vulnerabilities in their products that introduce cyber risk to U.S. households and enterprises.
- CISA should adapt the CPGs to include guidance to software and hardware manufacturers to follow the secure-by-design and secure-by-default principles and approaches created by CISA.[13]
- Promote greater use of checklists by auditors. CISA should encourage the inclusion of these broadly and through the CPGs to elicit more board engagement and accountability.
    - Auditors create checklists based on regulatory frameworks, including some of the newer ones described in this report. These checklists can include questions on how boards conduct themselves and how management reports to the board on cybersecurity matters (e.g. "Does your CISO report to the board?" or "Are they a member of an Information Sharing and Analysist Center (ISAC)?").
- Greater clarity on due diligence and liability. In addition to efforts to support the adoption of the CPGs as the common set of controls for publicly traded companies, CISA should create guidance for directors on what constitutes due diligence when it comes to cybersecurity.
- CISA should help define for boards and management the legal frameworks to help them navigate personal and organizational liability issues.
- CISA should simultaneously work with relevant federal agencies and stakeholders to determine what barriers exist to shareholders' pursuing class action lawsuits against companies for weak cybersecurity programs that result in harm to them or their customers.

Pillar IV: Sustained Leadership and Collaboration

Dedicated, high-level CISA leadership and stronger interagency and cross-sector collaboration are needed to augment awareness, knowledge, and governance abilities among the stakeholders of corporate cyber governance. We must foster more regular, authentic stakeholder interaction around the challenges of creating cyber resilient corporations that enhances learning and standards development but provides corporations with tools and information that helps them meet their own unique structures and needs.

- Assign a high-level leader and staff. As soon as practicable, CISA should designate an official under its Cybersecurity Division (CSD) to lead a line of effort around increasing national corporate cyber responsibility.
    - This individual should be high-level and should have previous industry experience, either as a former board member or former CISO reporting to a board. This person shall have, as one of their ongoing responsibilities, the evaluation of CISA's overall efforts relating to corporate cyber responsibilities, as recommended in this report.
    - CISA should assess the number and level of personnel required to implement the accepted recommendations in this report and dedicate these full-time equivalents to this line of effort, reporting to the aforementioned leader. To assist with the LOE, CISA should take advantage of industry expertise by leveraging rotational programs such as the Cyber Innovation Fellows or the Loaned Executive Program.[14]
- Create an awareness campaign.
- CISA should create an awareness campaign to encourage a nationwide culture of corporate cyber responsibility. Through this campaign, CISA should solicit feedback from relevant stakeholders and promote the resources it and its partners have created to foster and enable stronger board engagement.

[13] https://www.cisa.gov/securebydesign

[14] https://www.dhs.gov/loaned-executive-program#:~:text=The%20Loaned%20Executive%20Program%20is,security%20challenges%20through%20the%20Program.

Appendix A: List of Contributors to this Report

The following CCR subcommittee members participated in the study and recommendations documented in this report.

Dave DeWalt, Subcommittee Chair, NightDragon
Vijaya Gadde, Former Twitter
Ron Green, Mastercard
Cathy Lanier, National Football League
Ciaran Martin, Former National Cyber Security Centre
Ted Schlein, Kleiner Perkins
Alex Stamos, Krebs Stamos Group
Kevin Tierney, General Motors
Alex Tosheff, VMware
Chris Young, Microsoft

DRAFT REPORT TO THE CISA DIRECTOR

Turning the Corner on Cyber Hygiene

September 13, 2023

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Turning the Corner on Cyber Hygiene (CH) Subcommittee to examine how the federal government and industry can collaborate to identify appropriate goals and ensure strong cyber hygiene is easy to execute. To prevent a "boil the ocean" scenario, the subcommittee narrowed their focus to three sectors: K-12 public education, hospitals, and healthcare, and water supply/delivery/treatment. These areas of focus coincide with the Department of Homeland Security and White House objectives for defending the systems and assets that constitute critical American infrastructure. The CISA Director tasked the Committee with advancing the following scoping questions:

1. How can we encourage technology companies and software providers to develop products that are secure-by-design and secure-by-default to move the burden of security away from small and medium enterprises?
2. What specific actions should we recommend, that will materially improve technology product safety, and how do we best communicate these in a way that resonates?
3. What is the best way to evaluate progress toward all technology manufacturers building safety into their technology products?
4. How can CISA best support "target-rich, cyber-poor" entities in these sectors?
5. Which services and resources will make the most difference, and how can we most effectively measure a reduction in risk to these entities?

Findings

The subcommittee engaged in a series of discussions with industry and sector panelists and experts to inform the Committee's tasking. Briefers shared feedback, concerns, and insights with the subcommittee, bringing details about the challenges that exist towards becoming secure. It became clear that due to entities varying in levels of size, complexity, and maturity, there is no "one size fits all" solution to apply. For example, the healthcare sector has many different government agencies, at both a federal and state level, that provide oversight. This is compared to the K-12 education sector, where there are minimal cybersecurity capabilities and partnerships between federal and state governments and school systems. Throughout the sector discussions, the subcommittee regularly heard the idea that it is easier to maintain cyber hygiene within larger, well resourced, well-tuned service providers and systems. It becomes a more challenging situation at smaller institutions with legacy systems and technology. According to Andrew Hildick-Smith (WaterISAC), 10,000 of the largest 143,000 Public Water Systems (PWS) provide water to 90% of the U.S. population, yet only a portion of those PWS have operational technology (OT) that is at risk to cyber-attacks. The threats are not just focused on OT specific to that sector, rather the majority of the cybersecurity incidents that occurred since the beginning of 2021 were ransomware attacks. Successful OT attacks were almost as common as successful information technology (IT) attacks and compromises. With the majority of PWS being smaller, they are not well positioned to defend against the most basic IT security threats. After speaking to the health, water, and education sectors, a pattern of issues that were common in the sectors was identified:

Lack of Authoritative Guidance

- There are no reference architectures or easy to use best practices documented and followed within or across the sectors.

- For those who are making investments into partners to assist, as they do not inherently understand cybersecurity, there are no resources to know whether they have invested in a good security program or service provider or a bad one. There is nobody saying, "you have done the right thing" in these circumstances.
- There do not seem to be any collaborative arrangements across groups of utilities or service providers, those with the ability to influence and support with their expertise or experiences do not have a reliable way to engage others in the sector needing such support.

Lack of a Path Towards Funding

- Cybersecurity investment is lacking as it is rarely viewed as a top priority for spending.
- It is rare to have a dedicated budget focused on improving the security posture of their organizations, therefore progress is often made when combined with other deliverables or value add-ons.
- Cybersecurity grant programs along with state revolving loan programs primarily exist at a regional or state level but sector entities may operate across regional or state boundaries.
- Raising water rates or costs to the consumers to incorporate cybersecurity as a normal cost of business is not simple, due to regulations and oversight of utilities providing public services. You simply cannot pass on the costs as you would in a more commercial private sector situation.

Lack of Expertise

- Cybersecurity skills are often seen as something unique to normal subject matter expertise in the sectors. At best, perception is that this is an extra area of focus or work that needs to be absorbed along with other primary roles and responsibilities.
- There is not a wide range of staff resources available. Sometimes, a single individual is put into a position to do everything.
- Due to a lack of IT staff, many utility companies outsource their IT work and consider it complete, regardless of if that IT outsourced partner has the cybersecurity skills or not.

Recommendations

Our recommendations include focusing CISA's resources on providing guidance in four areas: security foundations (secure-by-design), road mapping financial assistance towards a more secure future, technical support during exploitation, and security related technical expertise. CISA should increase their velocity, become the authoritative voice for cybersecurity in the United States, and focus on reaching out to the widest audience possible. Furthermore, CISA should identify and publicly share performance targets that illustrate success.

The subcommittee has observed CISA independently taking action in the following areas:

- Director Easterly and FEMA's Deanne Criswell Announce $375M in Funding for FY23 State & Local Cybersecurity Grant Program.
- CISA publishes K-12 cybersecurity roadmap.

- ***CISA serves as the unifying voice for security guidance.*** Because of the role that CISA holds within the US Government, one that is focused on collaboration and influence with interagency partners, CISA should find unique and creative collaborations to advance its primary mission. Many agencies and organizations (e.g., Office of the National Cyber Director, Cyberspace Solarium Commission, Departments of Education, Health, Environmental Protection Agency, etc.) find themselves coming to similar conclusions around how to protect critical infrastructure and CISA should take a lead role in blending these ideas and strategies together in a singular vision and voice that allows both private and public sectors to achieve meaningful security outcomes.

- ***Define sector specific communications that are themed around "Understanding My Risk & Readiness".*** Create accessible, easy to understand, discoverable, yet authoritative, security guidance to address actual sector risks.
  - The materials will have real world user stories, and security best practice examples of fixes.
  - CISA should search far and wide for examples of best practices, pilot programs, and opportunities for increasing understanding.
  - Clearly define the threat landscape, allow for quick risk assessment, and quantify if the existing risks are relevant to Americans working in the three critical sectors. Sector members need to be able to answer the following questions quickly and correctly: "What threats should I be wary of?", "Now that I understand my risk, am I vulnerable?", and "Based on what's happening out there, what's the likelihood that it's happening to me?"
  - Highlight the importance of multi-factor authentication (MFA), end of life (EOL) software removal, patching, etc.
  - These vignettes will see the threat and attacks from the impacted parties' perspective, and highlight the warning signs, things to watch out for, and call outs for each stage of the attack on what preventable measures would need to be in place to prevent the attacker from being successful.
- ***Create a roadmap to action to overcome financial barriers.*** Most of the health, water, and education sectors want to be secure, but simply do not know how. They lack the first steps and are often deterred by the financial barriers to entry. CISA must highlight a path to financial assistance.
  - Answers must be provided to the following questions, "Where does one turn to get the financial resources needed to be secure?", and "How does one position trade off and prioritization decisions that put security needs first?"
  - Once someone decides to make the investment in security solutions or service providers, CISA should publish tips and tools to identify effective IT / cybersecurity partner companies that will be successful in assisting via outsource arrangements.
- ***Establish key security metrics.*** You cannot fix what you do not measure. In an effort to establish a more secure future, companies need to know how they measure up in the security landscape.
  - CISA needs to establish key security metrics that allow the sectors to know if they are making meaningful and effective security changes that reduce their attack surface.
  - Data on its own is not enough, performance indicators per sector should have context and take data and turn it into information that allows operators and sector businesses the ability to make new and informed decisions on the security posture of their companies.
  - These security metrics will be published by CISA to find common language across sectors to show the current health of an institution and to illustrate if they are indeed able to deliver on intended security outcomes.

The recommendations outlined above are the initial steps in a long journey toward securing the American public and businesses.

Appendices:

The following Turning the Corner on Cyber Hygiene subcommittee members contributed towards this report:

- George Stathakopoulos, Subcommittee Chair, Apple
- Marene Allison, Former Johnson & Johnson
- Steve Adler, Former Mayor of Austin, TX
- Brian Gragnolati, Atlantic Health System
- Royal Hansen, Google
- Doug Levin, K12 Security Information eXchange (K12 SIX)
- Ciaran Martin, Former National Cyber Security Centre
- Nuala O'Connor, Walmart
- Matthew Prince, Cloudflare
- Robert Scott, New Hampshire Department of Environmental Services
- Alex Tosheff, VMware

DRAFT REPORT TO THE CISA DIRECTOR

National Cybersecurity Alert System

September 13, 2023

Introduction:

The Deliverable (from CISA 2022 tasking memorandum)

"The CISA Cybersecurity Advisory Committee (CSAC) will produce a report to the Director that will describe the needs, benefits, and operational efficacy of a National Cybersecurity Alert System."

Background:

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. As part of its cybersecurity mission, CISA coordinates the execution of US national cyber defense, leading asset response for significant cyber incidents and ensuring that timely and actionable information is shared across federal and nonfederal and private sector partners. This includes analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

> Current State. CISA oversees the National Cyber Awareness System which offers a variety of cyber defense information for users with varied technical expertise. This system produces advisories, alert and situation reports, analysis reports, current activity updates, daily summaries, indicator bulletins, newsletters, recommended practices, a Weekly Analytic Synopsis Product (WASP), weekly digests, and year in review to alert partners of emerging cyber threats, vulnerabilities, and risks. However, these various alerts and advisories do not provide an easily understandable sense of national cyber risk, a characterization of granular changes in the risk environment, and/or continuous coordination among the various federal entities performing similar functions in the present day.
>
> Topic for Study. CISA is interested in understanding the feasibility of an alert system for cyber risk. The goal of this capability would be to provide a clear and simple method to convey the current severity of national cybersecurity risk based upon CISA's all-source analysis of evolving threat activity, such as through a color-coded or numerical "scoring" system. Such a system would complement rather than replace CISA's existing production of alerts and advisories on specific, actionable risks.

Specific questions for the CSAC to address (the "seven questions" from 2022 tasking memorandum):

1. Assess the need for a "National Cybersecurity Alert System" and the specific gap to be addressed.
2. Consider whether CISA is the right agency to provide this type of capability and whether CISA should partner with other federal departments or agencies to be most effective.
3. What should the alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to these cyber threats?
4. Determine the criteria or situations which need to be considered for such a system, to include risk.
5. Identify how CISA could measure the effectiveness of this new capability.
6. Identify a platform or mechanism to ensure there is widespread awareness regarding this capability to ensure it is effectively leveraged.
7. Are there lessons that CISA can leverage from non-cyber national alert systems such as the Federal Emergency Management Agency's Hurricane Alert System and DHS' National Terrorism Advisory.

Additional (amplifying) CISA Guidance from NCAS subcommittee Chair Discussion with CISA Leadership on 12 May 2023:

- CISA is looking for ways to improve the fidelity and sustainability of the current system – one that is more tightly coupled to current conditions and trends.
- The 2022 "Shields up" program combined specific, time-delimited, warnings (ex, "threats are significant and imminent … defenders should lower threshold for sharing *now*") and enduring (general) cyber security guidance (ex, routinely patch, use MFA, enhance segmentation, etc.)
- Emphasis in the proposed national cybersecurity alert system should be on the former.
- CISA expects a small number of recommendations from the Committee.
- The seven framing questions remain valid, but can be expanded as the Committee sees fit.
- A defined role for industry will be important.
- CISA needs a framework and vernacular with which to engage industry.
- A Final Report with recommendations by September 2023 is preferred.

Findings

Question 1: Assess the need for a "National Cybersecurity Alert System" and the specific gap to be addressed.
Discussion:

National Cybersecurity Alert System Contours: There is clearly an appetite for, and a perceived gap in, servicing the expressed interest, on the part of the vast majority of the CSAC NCAS subcommittee and the various private sector interlocutors the subcommittee engaged over the course of the study (see Appendices 1 and 5). Many reflected on the value of CISA's 2022 "Shields Up" campaign, noting that it provided a valuable emphasis on creating awareness of heightened cyber threat, and in providing justification for increased security measures, even if it lacked desired specificity in timing, focus and granularity.

Pulling from lessons identified in the 2009 Homeland Security Advisory Council (HSAC) Task Force report on the Homeland Security Advisory System (see appendix 10), other U.S. Government conditions or alert levels (FPCON, etc.), and inherent differences or limitations in cybersecurity vice other security disciplines, we can define the general contours of a prospective national cybersecurity alert system consistent with CISA's requirements (not accounting for or assessing feasibility under this question). An 'alert' should delineate:

- **Sub-national, Group Specific:** The 2009 HSAC Task Force report made clear that an alert at a national level (without specifics or reference to a target group, region, etc.) is too vague to be useful or actionable. It also noted that in any incident that is significant enough to be a truly national-level issue, an alert system would be useful and likely beaten to the punch by news media.

- **Defined Timeframe of Applicability:** Any "alert" or change in condition would need to define the timeframe in which it is applicable or active. At the end of a timeframe it should be renewed, allowed to expire, or amended.

- **Routinely "Normalized" Baseline:** Any alert system would need to routinely define the assumed "baseline" of threat and risk for a given group for which baseline guidance and short-term, time-limited, measures might be suggested. A sustained threat would thereafter cease to be an alert but incorporated as an element in a baseline "normalized" condition. This would encourage enterprises and business to routinize and optimize security and defense for the specific threat or vulnerability as a matter of standard operating conditions, rather than an unsustainable enhanced readiness/vigilance/increased security posture. Baseline condition would be "no unusual or heightened activity". This is drawn from how FPCON defines its base state and is intended to address a few key concerns raised by the HSAC Task Force in 2009, namely the political issue of reducing the alert level and continuing to maintain heightened or increased risk in an environment where a baseline level of risk is neither defined or assumed as enduring and standard.

- **Condition Set by Likelihood of Targeting or Exploitation:** Existing alert systems inform CISA customers of newly discovered vulnerabilities, indicators of compromise (IOCs), and, on occasion, victim notification. This tactical information is complemented by largely yearly products produced by information sharing and analysis centers (ISACs), the Office of the Director of National Intelligence (ODNI), and CISA on assessment and forecasting of specific threat actor groups.

- **Information at the operational level** is a key missing piece, particularly assessments of threat actor behavior in the day, week, or month timeframe (identification of changes in targeting preferences, new campaigns, etc.)

    - This is a necessary piece in assessing and alerting the likelihood of targeting or exploitation (to detect and mitigate or prevent entirely) for a specific group or at a national level (where applicable) within a defined timeframe.

While the classic definition of "risk" is a function of threat, vulnerability, and consequence, the subcommittee suggests that alerting a specific group that they are likely to be at risk or are targeted (or are already) is the most useful component of system that collects and disseminates risk information. Risk must define the target audience, not merely the threat actor or venue.

Overall Assessment: A national cybersecurity alert system would be a useful service, if executed with rigor, a high threshold for actionability and relevance, and with sufficient supporting intelligence and analysis to be routinely useful. The effort must be given as a primary task to an organization that dedicates full-time resource and focus to the task.

The alert system itself would be useful, no doubt, but its real value would be in the process, capabilities, discipline, and tradecraft that would need to be built in order to field it. Ultimately, the national cybersecurity alert system implicates an enduring question plaguing CISA, and an existential one: What is the business model? What is the value-added and to whom? Key points are captured in the Findings below.

Finding 1: There is a **genuine need** for a national cybersecurity alert system that routinizes the 24/7 consideration and provisioning of cyber alerts and, when possible, guidance to organizations and persons in a position to take action to mitigate identified risk(s) (through a variety of means that include bolstering defense, risk reduction measures, and reducing exposure).

Target groups can be defined using sector, region, size, maturity, and technology for which alerts should:

- Be time-defined or limited (alert levels would then be “normalized”, “extended”, or “reduced”).
- Be based on risk of targeting (or having been targeted) by a threat actor or risk of having an exploited (or likely to be exploited) vulnerability.
- Provide guidance in the initial state change; with additional guidance issued when alert is normalized, extended, or reduced.
- Be informed by and operate alongside existing CISA alerts, advisories, and reports and, where possible, integrate other federal agency products.
- Include a formally defined means to review, alter, or revoke the alert.

Question 2: Consider whether CISA is the right agency to provide this type of capability and whether CISA should partner with other federal departments or agencies to be most effective.

CISA’s implementing statue(s) and relevant executive orders (most notably PPD41) clearly place CISA in the lead role and it would be difficult to argue that any other federal agency is in any better position to take this on. Of note, private sector comments on the national cybersecurity alert system task (see appendix 5) stated that “*The US government has a unique opportunity to synthesize and disseminate threat information that enables disruption of active threats.*” While this aspiration goes beyond a purely national cybersecurity alert system function to imagine a systemic mechanism by

which those *alerts* might feed a whole-of-nation effort to *disrupt* cyber threats, it nonetheless highlights the unique position occupied by the government to convene, facilitate, and coordinate nation-wide, cross sector cyber alerts.

CISA's current ad hoc cyber alert and warning system (described as the National Cyber Awareness System) is composed of tactical level "alerts" (notifications of new actions or news), advisories (longer-term reporting of threat campaigns, IOCs, and severe vulnerabilities). The current system is complemented by vulnerability notifications and victim notifications, which are time-consuming, resource intensive, and difficult to scale**.** That valuable foundation notwithstanding, CISA's current capabilities lack:

- Continuity (a 24/7 focus on warning and alert functions);
- Standardization (use of common, widely understood terminology) of terms like "alert", "advisory", and "bulletin" both in how they are used within one organization (CISA's use has shifted or is amorphous over time) or across the federal government.
- Integration or incorporation of other federal agency alert systems beyond "joint cybersecurity advisories" between CISA, FBI, NSA, and others.
    - Any national cybersecurity alert system would need to track, be aware of, compile, and analytically incorporate federal products into a common risk assessment for an "alert" or state change related to a group.
- Defined timeframe of an alert or advisory (i.e., when it is normalized, or a period of risk has ended).
    - Prescribed revisits of a given warning or alert that provide opportunities to reduce the wear and tear that comes from extended periods of defensive surges that are not based on sustained threats.
    - There is a lack of connectivity and coherence across the various federal and private sector organizations that comprise today's ad hoc alert and warning system.
- Lack of Insight on Cyber Environment, Customer Networks, and "TechStack"
    - Understanding how a threat assessment/likelihood of targeting or exploitation applies to a specific group requires detailed knowledge of the group in question. Currently, CISA has limited or inconsistent/piecemeal information on common technologies, vendors, lines of business, etc. across enterprises within regions, sectors, or sub-sectors— a key data point in trying to determine the scale or pervasiveness of a problem for newly-discovered, severe or critical vulnerabilities.
    - Additionally, beyond what is publicly registered, CISA does not have direct or easily accessible information on ownership of internet selectors like IP addresses— limiting its ability to provide victim notification or indicators and warning to a specific enterprise through threat actor telemetry. CISA does possess administrative subpoena authority to order telecom companies to identify the owner of a specific IP address, but this process is not scalable or particularly useful in developing warnings/notifications of imminent threat.
    - There have been efforts to identify common technologies for certain sectors (e.g., Financial Services), but these have relied on a voluntary process that is uneven and incomplete. There have been other efforts to solicit technical selectors on their IP space for use in I&W and tipping and queuing from critical infrastructure (i.e., Section 9 companies) in a more systematically way, but this has run afoul of perceived legal hurdles and competition with sector specific agencies which are sometimes the exclusive point of engagement for private sector entities.

- Lack of Analytical Capability and Programs - CISA lacks a dedicated standing threat intelligence analysis capability at a scale necessary to support a national cybersecurity alert system (assuming data is even available). Whether such a capability is suffused with sufficient (thus increasing amount of data to compile and assess) or a dearth of analytic capacity (thus requiring making up through inference what can't be determined directly), CISA's current resources, are insufficient in quantity and lacking in specialized areas of expertise (regional threat actors) and analytical tradecraft. CISA could outsource analysis to a third party, like a federally funded research and development center (FFRDC), the Intelligence Community (IC), or another contractor; augment their existing capabilities with in-house contract support specialized and targeted to fulfill skillsets or areas of expertise they currently lack; or forge a coalition of federal and private sector entities that collectively and collaboratively generates needed capacity.

On the matter of which, if any, federal partners CISA should work with to implement a national cybersecurity alert system, the Federal Bureau of Investigation (FBI) is perhaps the closest in possessing capabilities that would make a national cybersecurity alert system viable, by virtue of its geographically distributed network of field offices, an impressive and growing cadre of cyber threat analysts, and a rich feed of relevant threat information (via relationships cultivated by its field network, overseas liaison, and the Internet Crime Complaint Center (IC3) incident reporting system) but it faces limitations similar to those faced by CISA in terms of private sector reporting, available intelligence and the FBI's own ability to publicly post alerts that are sometimes limited by competing priorities of needing to maintain confidentiality for law enforcement operations and/or needing to inform stakeholders to prevent, prepare, or preempt an imminent threat. Appendix 6 ("Overview of U.S. Government Primary Cyber Alerts and Advisories") lists other organizations – not least of which the National Security Agency (NSA)'s Cyber Security Directorate—that are potential candidates for inclusion into a federated approach to implementing a prospective national cybersecurity alert system.

With or without federal partners, CISA would require increases in resourcing, focus, and organization.

Fielding a robust national cybersecurity alert system as articulated above (with tactical-level products and operational-level alerts) that is useful and credible would also require a transformation and refocus of some portion of CISA's core business model— which has largely been defined by assessment of generalized, all-hazards "risk" and tends to be indexed by vulnerability and consequences rather than threat.

In particular, this prospective new model would need to prioritize data collections, analytic tools, analysis capacity and tradecraft, and more targeted, scalable solutions over resource-intensive operations that produce marginal value in data or intelligence terms (incident response, threat hunting, risk and vulnerability assessments, and technical indicator identification), outsource them to sector specific agencies as appropriate, or do away with them entirely.

Finally, while CISA is clearly the most logical choice for leadership of a national cybersecurity alert system capability, the opportunity to leverage the unique capabilities and relationships of the FBI and various Sector Risk Management Agencies (SRMAs) must be seen as both a means to mitigate CISA's current resource deficiencies and to greatly strengthen the capacity and coherence of a US federal effort that serves the collective needs of the private and public sectors for a national cybersecurity alert system .

Finding 2: CISA is the right federal entity to further define and lead the development and implementation of a national cybersecurity alert system.

Finding 3: CISA does not currently possess a framework and supporting organization dedicated to nationwide cyber threat analysis whose goal is to support real-time alerting to defenders. CISA currently lacks analytical capacity and unique, value-added data sources to be able to reliably field a national cybersecurity alert system.

Finding 4: The forthcoming implementation of the 2022 CIRCIA offers CISA a unique data source on current incidents, which can be combined with other government and private information steams to yield a more routine, granular and coherent understanding of threat and/or vulnerability activity.

Finding 5: Additional work in defining SIEs (finding common technologies, lines of business, etc.) and identifying cross-sector enterprises that rely on common or similar TechStacks (i.e. industrial control system (ICS) for utilities, etc.) can be useful in assessing risk and defining groups that may share risk, but the work may be slow and hard to scale.

- **Course of Action #1: No national cybersecurity alert system** - CISA could elect to not pursue a national cybersecurity alert system. To be absolutely clear, a national cybersecurity alert system (as envisioned above) *could* be useful if sufficiently resources, sparingly used and only when credible and actionable, and tailored specific to those most relevant to its contents. But it is not a critical, make-or-break component— it can help optimize, prepare, and make more efficient and targeted periods of enhances security procedures. Existing CISA tactical alerts, IOCs, advisories (campaign-level), and vulnerabilities provide a steady stream of actionable content to enterprises. Though lacking in

context and intuitive method of quickly assessing its relevance, it is a baseline function that can help enterprises that are paying attention.

- **Course of Action #2: National cybersecurity alert system-lite** - CISA could develop a national cybersecurity alert system that only follows *some* of the criteria or key dimensions outlined above. It could, for instance, focus on issuing alerts and assessments reactively, only in instances where a campaign has been identified and disclosed (usually through advisories) or a particular severe vulnerability has been identified. What is most meaningful here is being able to tailor the alert and its distribution to particular groups or sets— that would still need to be maintained. However, shifting from predictive/forecasting to reactive alleviates the need for greater analytical capacity and larger quantities of data and threat intelligence. General alerts for specified groups would lack the total context of a full national cybersecurity alert system but would still provide some indication of relevance and priority absent in the current alerting system.

- **Course of Action #3: CISA-FBI national cybersecurity alert system** - CISA could partner with the FBI in fielding this capability; it is standard procedure for more operational-level or strategic "advisories" (usually outlining and disclosing an adversary campaign with associated IOCs) to be multi-seal, collaborative, and consensus documents jointly issued by multiple US agencies. CISA and FBI have been the core partners in these advisories (and have the longest-standing collaboration). A national cybersecurity alert system would be a natural evolution in this partnership. The challenges are many but, workable. Lack of communication between field offices and FBI HQ and competing priorities as noted above continue to plague this collaboration and would likely do so under a joint national cybersecurity alert system. Additionally, the lack of routine sharing of or access to each agency's raw data (particularly in FBI's case) puts limits on the extent of analytical collaboration. CISA and the FBI would have to work out decision-making and authority for alert issuance. It is likely that the contours, thresholds, "groups", distribution channel, and other key dimensions of a national cybersecurity alert system would need to be shaped by FBI as a condition of their participation and partnership. While this cedes some control from CISA in the design and stewardship of the capability, it is a worthy tradeoff for greater leverage of FBI threat information, analytical resources, and relationships (especially the cyber focused staffs deployed across its national and international offices).

- **Course of Action #4: Future national cybersecurity alert system** - The passing of the CIRCIA provides CISA a critical and unique capability, namely indicative if not comprehensive threat intelligence and incident-related data on an enduring basis (for critical infrastructure). This fills a much-needed gap for the agency and resolves its lack of a unique, scalable source of threat intelligence. CIRCIA is still in its rulemaking process, affording CISA ample time to both take full advantage of the information CIRCIA can offer and build-out capacity and capability necessary to make a national cybersecurity alert system viable, useful, and credible. In particular, CISA could build out its analysis capacity; develop or procure new analytical tools in a modernized infrastructure; develop qualitative metrics and threshold for a national cybersecurity alert system; and define workable, scalable ways to identify common technologies/interdependencies among sectors/regions that are useful in assessing scope of vulnerability impact. This course of action is not mutually exclusive with partnering with the FBI and, in fact, affords both agencies more time to work out kinks in governance, framework, joint systems, and information sharing— issues that are key policy and procedural questions in CISA's implementation of CIRCIA.

Question 3: What should the alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to these cyber threats?

Discussion:

Discussions with private sector cyber security professionals (see appendix 5) and with Israeli and UK CISA-counterpart organizations (Appendices 3 and 4) highlighted a compelling statement of need for such an alert system. The private sector discussants noted that the US government has a unique opportunity to synthesize and disseminate threat

information that enables disruption of active threats. Their comments framed the constituent components of a useful cyber alert system as:

- The alert system should:
  - Serve ONLY for the timely dissemination of urgent and actionable alerts that enable recipients to anticipate and prepare for specific cyber threats.
  - Optimize for cyber incidents that are ongoing or have recently happened and continue to produce damage, vulnerability, and potential harm.
  - Optimize the reporting pipeline to incentivize and accommodate high-fidelity, high-value cyber incident reporting sources. Speed and action ability will be an essential components.
- More specifically, the alerting system should emphasize creating mechanisms for:
  - Directly reporting to victims or their security vendors that can take actions.
  - Determining relevant **actioning stakeholders** (organizations or people that can take actions to mitigate harm or categorically disable attacker capabilities).
  - Inform the security practitioners at relevant verticals or affected organizations.
  - Use global broadcasting ability ONLY when absolutely necessary.
  - Define a clear value adding function that naturally incentivizes operators to involve CISA in order to reach a favorable outcome.
  - Focus on enabling action(s) that prevents, interdicts and/or disrupts threats.

The elements included in a given alert would vary depending on the imminence, focus, and scope of the given threat or vulnerability. Appendix 6 describes a Possible Framework for Cybersecurity Information by type and level, but any alert should include the elements identified above by the private sector security professionals engaged during this study, any relevant guidance on actions that may mitigate or prevent the threat identified by the alert, and a mechanism for reviewing the alert over time to adjust and/or terminate the alert based on changing conditions.

A national cybersecurity alert system would then seek to (using CISA's existing products and data), identify instances where a specific group is at heightened or imminent risk that they are or have been targeted by a threat actor group or have a known/discovered vulnerability that will be or has been exploited.

- **Feasibility Considerations:** The "national cybersecurity alert system contours" discussion under Question 1 of this report was generated assuming that CISA has - or can attain - capabilities necessary to be able to routinely issue relevant, actionable alerts and has sufficient data/intelligence to tailor it to a specific group and assess likelihood of targeting or exploitation. However, we need to determine the feasibility of CISA actually being able to field this capability. In this regard, CISA faces a series of considerable challenges and limitations, not only in the information available to it, but in its own analytical capacity, ability to share or incorporate data from external sources, and knowledge of technical and functional environment necessary to identify when a threat or vulnerability may be most applicable to a specific, tailored group.
- **Inherent Limitations of Cyber Threat Intelligence -** As opposed to counterterrorism, natural hazards, or other conventional domains, cybersecurity is critically limited in that it rarely has *direct knowledge* of the threat actor (i.e. direct surveillance or intelligence on adversary operations and decision-making) at a tactical level. Most knowledge is derived from technical information collected from incidents. Understanding the context of any one incident (and whether it is indicative of change/consistency in pattern of behavior or an anomalous data point) takes time through incidental discovery, time in assessing and linking multiple incidents, tying to a threat actor, and, finally, assessing or forecasting the significant of the behavior in the context of threat actor objectives, patterns of behavior, etc. This means that threat intelligence often lacks context, operates on a significant time delay (often but not always), and does not benefit compared to other security disciplines from the US's existing strengths in foreign intelligence collection. A compounding factor is that much of the data by which to make informed assessments are held by disparate cybersecurity, incident response, or threat intelligence firms— who have little incentive to share information that could diminish their competitive advantage relevant to their competitors.

- **Key Limitations on US Government Threat Intelligence -** The most obvious limitation on US government threat intelligence is the inability to deploy sensors domestically at scale— either to monitor general internet traffic or monitor the networks of specific enterprises. CISA has fielded some prototype capability through voluntary agreements, but it does not appear this program has been made a principal program and scaled to a level where necessary network effects can make it viable. Further, in instances where the government does place sensors on domestic networks (e.g., FBI sensors on compromised networks, Department of Energy (DOE)'s Cybersecurity Risk Information Sharing Program (CRISP)) the information is siloed and not routinely shared. Existing programs like Einstein-3A and Enhanced Cybersecurity Services have faced increasing ineffectiveness due to technological change (encrypted network traffic, move to cloud hosting by US government, etc.) or dearth of collection of classified indicators.
- **Ineffective or Absent Public-Private Threat Sharing -** It is unlikely the US government can persuade (or force) cybersecurity, or threat intelligence companies to share information they consider a trade secret. Previous attempts to remove barriers to sharing (e.g., prohibition on regulatory use, limited liability protection, etc.) have not been effective in encouraging sharing at scale. Programs like Automated Indicator Sharing (AIS) have seen less than expected participation by private sector partners and lack the context the private sector needs to appropriately determine the relevance, priority, and actionability of any given data point. It is unlikely this is a solvable problem in the near-term; CISA's focus appears to be in established trusted communications channels between targeted partners to coordinated operations and information person-to-person; rather than designing and fielding a technological medium for automatic tactical threat sharing and collaborative assessment (as reflected CISA's arguments against the Congressional recommendation in legislative year 2022 for a formally constituted *Joint Collaborative Environment*).

Defining target audiences is perhaps the most difficult portion of a national cybersecurity alert system implementation.

Alerts should be relevant and tailored to a specific group and, indeed, the accuracy and usefulness of any assessment is helped considerably by how focused/narrow the group being evaluated is. If the audience is too large, the benefits of an alert are diluted, lack precision, and lose relevance and influence over time. A sector-based grouping system is useful, intuitive, and has ready-made distribution channels via ISACs; however, it does not account for the incredible disparity in security maturity across most sectors— the size and maturity of an organization being a significant factor in targeting either intentionally or through opportunistic vectors.

CISA may find it advantageous to use one or more grouping definitions (that can be cross-cutting) that can serve to focus the alert, define to whom it applies, and guide targeted distribution. Risk would then need to be assessed by the groupings together rather than individually. There are a few key grouping types that should be used (though there are many, these are selected for their intuitiveness and simplicity):

- **Sector or Sub-sector -** The most identifiable grouping, with a ready-made distribution network, and routine assessment of group-wide risks and threats. It is not enough on its own, however, as even within critical infrastructure (CI) sectors, there are a number of other significant factors that weigh into a threat actor's targeting preferences. Additional detail/distinctions need to be made.
- **Criticality -** Sector or sub-sector presumes critical infrastructure, but an additional field to specify critical is useful when an alert only applies to SIEs/SICIs or in instances where an alert may be more general and apply to all enterprises irrespective of their specific criticality (i.e. there is no specific sector or sub-sector to be defined).
- **Region or Locality -** Likely a rarely used field, it may nevertheless crop up from time-to-time, particularly with criminal actors that have a regional preference or areas where a sector or sub-sector is concentrated (DC and Government, New York and financial, etc.), or activist/localized campaigns targeting a specific municipality.
- **Technology "Clade"** - CISA has done some general definition to define enterprises by their technology stack, making a distinction with ICS alerts versus more general IT-focused ones. There may be more to be done here, to identify groupings of businesses that share network architecture, equipment and device type, and services in common - and thus have a similar risk profile re: vulnerability. ICS/OT is a good distinction, one that walks a fine line between being broad enough to loop in a significant portion, but not too broad as to dilute relevance of any given alert. It is also intuitive. Something like "Microsoft Office users" maybe too narrow. Other clades could

include Home or Small Enterprise (COTs devices, few firewalls, no on-premises, personal device use), Development Environments (software developers, etc.). More research is needed on this, but the subcommittee believes that groups sharing common "stacks" can be identified at a similar scope and would be a useful distinction to make.

- **Mission or Business Activity -** It may be worth having an additional distinction on mission or business activity. For example, for Chinese threat actors pursuing China's research and development (R&D), science and technology (S&T), and economic development goals through IP theft sending alerts by defined by sectors (Academia, Defense Industrial Base, etc.) may be too broad to be useful and is not the principal way the actors would define their target set. It would be by mission or business activity. "Quantum Information Science", "Artificial Intelligence Research", "Stealth and Meta-material Development", would be more useful and better aligns to the commonality between different enterprises that is the reason for targeting. Similarly, distinctions such as "Utilities" are inherently cross-cutting and are more accurate and efficient distinction for certain types of threat actor targeting preferences than simply saying "Electric", "Water", etc. There needs to be some research on a mutually exclusive, comprehensively exhaustive taxonomy (for consistency and to ensure differentiation/distinction with sector and sub-sector groupings) but that's beyond the scope of the study.

Question 4: Determine the criteria or situations which need to be considered for such a system, to include risk.

Regarding possible Levels and Risks Calculation - There was general consensus among public respondents to this study, and from HSAC Task Force members in its 2009 study, that any alert system should hew to the use of specific language and avoid using colors or other broad 'labels', both because it does not capture the full context/message that needs to be conveyed and it draws and unhelpful and unfortunate connection to the poorly regarded former terrorism alert system.

- The current National Terrorism Advisory System (NTAS) uses simple descriptors (heightened, elevated, etc.) rather than colors or numbers.

- CISA *could* attempt to define some quantitative method to define risk (or likelihood) of targeting within a defined timeframe for a given group, but we would suggest that there are too many unknown variables at play to arrive at a satisfying and consistent method that would have enduring credibility. A more qualitative method may be more useful and efficient and less subject to false certitude that can lead to overconfidence and critical errors.

- Existing frameworks to assess the severity of newly discovered vulnerabilities are extremely useful as a data point, but they do not speak to a vulnerability's pervasiveness within a given group or the likelihood and degree it will or has been exploited by threat actors. That additional information needs to be included and should be assessed qualitatively.

- The National Cyber Incident Severity Schema (NCISS) and other similar frameworks for evaluating severity or impact of an incident, while great tools for emergency management and incident response, are not applicable, here. They only speak to the severity and significance of an incident after-the-fact, not the likelihood of targeting of a specific group or exploitation of a vulnerability.

Regarding Content and Distribution - Similar to the NTAS, the national cybersecurity alert system should take a two-channel approach. This includes: 1) a short, publicly-posted "blurb" or "card" that summarizes the key details of the alert or heightened condition, who it is relevant to, and other top-level relevant factors; for National Terrorist Alerts there is usually an attachment or document with additional guidance or detail *for public consumption;* and 2) direct notification or distribution to participating members of the identified, relevant group, accompanied with additional detail, guidance, etc. that were not (or could not) be included in public versions.

Regarding Threshold - CISA has to maintain a delicate balance. Given the amount of activity in cyberspace, it would be ideal if CISA had sufficient data to be able to generate these insights *only* in instances where a threat or vulnerability is

truly widespread, has a high likelihood, and contains actionable information. Without a lot of data to be able to achieve this, there could be a tendency to reduce the threshold to increase the number of alerts (resulting in scope or "threshold drift"). This would lead to a downward-trending dynamic where alerts are diluted and are not meaningfully distinct from the tactical-level alerts CISA already generates. To engineer against this natural dynamic, the threshold decision-making authority should be placed at a high-level (CISA Director, Deputy Director, etc.) and should be evaluated against a set of rigorous qualitative metrics and benchmarks to be considered and actioned.

Finding 6: Alerts must be specific, targeted, actionable and subject to periodic review to ensure they remain current or are adjusted and/or terminated in a timely manner.

Regardless of the choice made for or against tiering, the CISA national cybersecurity alert system Team should rigorously consult with Sector Coordinating Councils, federal partners, and foreign counterparts on the characteristics of the proposed national cybersecurity alert system.

Question 5: Identify how CISA could measure the effectiveness of this new capability.

The mere **existence** of credible alerts, actionable information and attendant guidance on how recipients can better prevent or respond to cyber threat is a measure of effectiveness in and of itself. **Coherence** of federal efforts to solicit, synthesize, and disseminate cyber alerts is an important secondary measure that will deliver needed efficiency and optimal results in a system that is inherently heterogeneous in needs and capabilities.

Question 6: Identify a platform or mechanism to ensure there is widespread awareness regarding this capability to ensure it is effectively leveraged.

Identifying organizational responsibility (within the federal government) and the role of nonfederal stakeholders (private sector and CISA international counterparts) will be as important as identifying the platform, mechanism, or process.

Finding 7: The lack of an agreed-upon framework to assess risk across a defined group (e.g., sector, region, size, maturity, and technology "clade") under such a national cybersecurity alert system is a significant barrier to implementation. Existing systems like the National Cyber Incident Scoring System (NCISS) or National Cyber Incident Severity Schema are useful starting points but are intended to assess severity of an *incident* rather than risk of a particular threat actor or vulnerability's impact on a specified group and would need to be modified and adapted to generate a new alerting level schema.

Question 7: Are there lessons that CISA can leverage from non-cyber national alert systems such as the Federal Emergency Management Agency's Hurricane Alert System and DHS' National Terrorism Advisory System

After examining both the frameworks for the National Weather Alert System and the US Terrorism Alert System (a more detailed assessment can be found in appendices 8 and 9 of this report), each are intuitively appealing, yet perceived similarities are offset by distinct differences in the nature of both the threat and its impact. As noted in the discussion under Question 1 of this report, lessons identified in the HSAC Task Force report on the NTAS in 2009, other US government conditions or alert levels (FPCON, etc.), and inherent differences or limitations in cybersecurity vice other security disciplines, can help define the general contours of a prospective national cybersecurity alert system consistent with CISA's requirements (not accounting for or assessing feasibility under this question).

Finding 8: Previous experience with terrorism alerts suggests that the viability of any national cybersecurity alert system requiring nonfederal entities to provide or act upon information that affects their operating efficiency and/or liability to shareholders, regulators and customers will depend on a mix of incentives and liability shields to encourage private sector participation in generation of information underpinning alerts.

Recommendations:

- CISA should assign the task of developing a national cybersecurity alert system to a dedicated team ("CISA national cybersecurity alert system Team" equipped with the authority and resources needed to define, implement, and lead an operational national cybersecurity alert system.
    - In implementing this action, CISA should avoid simply utilizing existing distribution lists for alerts and instead take the opportunity to enhance its understanding of the intended customer set - filling in key gaps in its knowledge of the cyber environment. In any "sign up" campaign for the national cybersecurity alert system (not the tactical level alerts, advisories, and guidance, but the direct-to-group operational-level change in their risk condition), CISA should include a questionnaire with basic questions on sector, sub-sector, region, and business activity (group distinctions above) by which it can automatically tailor and distribute alerts in the future. Another consideration is limiting enterprises or organizations (at the lowest discrete legal entity-level) to one account (with multiple distribution emails/points of contact) to avoid conflicting or erroneous information.
- The CISA national cybersecurity alert system Team should initiate its work by identifying and working with stakeholders to define the purpose(s), formats, target groups, and measures of effectiveness for cyber alerts.
- The CISA national cybersecurity alert system Team should develop and implement a federated model for the national cybersecurity alert system that leverages authorities, capabilities, and infrastructure across the federal government and its counterparts in the private sector – the Committee offers several courses of action here but strongly recommends one that partners with the FBI organization leading threat response under PPD41 and with sector specific agencies leading sector cyber engagement.
    - In conjunction with ODNI and NSA, the CISA national cybersecurity alert system Team should review processes and procedures specific to the U.S. Intelligence Community CRITIC process (IC Directive 190) to include the newly established Intelligence Community Cyber Threat Alert, to determine whether that process is relevant or should be integrated into the national cybersecurity alert system.
    - In conjunction with FBI and other relevant partners identified under PPD41, the CISA national cybersecurity alert system Team should consider and implement one or some combination of the following four distinguished courses of action (COAs). Each one makes a tradeoff on key dimensions of an optimal national cybersecurity alert system: need, quality, control, and timeframe. CISA should follow COA 3 with a view to enhance that approach using COA 4 as time and circumstances allow.
- The national cybersecurity alert system should consider a tiered release strategy that provides most timely and granular information to those with largest equity and ability to action the information-in-question on behalf of the broadest population of downstream users. Ring 0 covers warnings that are imminent and specific. A possible tiering strategy (the timeliness requirements are loosened, and the audience expands as the tier number increases):
    - Ring 0: Targeted entities for imminent warnings that are specific and/or significant in impact (concurrent with cc: to affected SRMAs).
    - Ring 1: Affected entities for non-imminent or non-specific threats (e.g., multiple/cross-sector threats or a technology in wide use).
    - Ring 2: Relevant SRMAs and ISACs for sector specific alerts, warnings and/or guidance.
    - Establish process to coordinate development and release of alerts, warnings, and guidance to FBI's National Cyber Investigative Joint Task Force, NSA's Cybersecurity Collaboration Center, SRMA's, and ISACs.
    - Provisions should be made for delegated authority to NSA, FBI, SRMAs, and ISACs that ensures the right alignment of efficiency and coherence.
    - Getting actionable alerts from numerous entities might undermine the actionable nature of seemingly contradictory alerts.

  - Consideration should be made whether it is better for there to be only ONE entity that sends out the Alerts– in particular Ring 0 alerts. **NOTE**: The Israeli model centralizes responsibility for cross-cutting and critical alerts to the central authority.

- The CISA national cybersecurity alert system Team should build on existing CISA monitoring processes and associated National Cyber Incident Scoring System (NCISS) to add *warning*, *alert*, and *guidance* functions (that yield the so-called national cybersecurity alert system) that ensure this knowledge is leveraged for the benefit of cyber users. Definition of these terms follow:
  - Warning: information reflecting expected imminent threats (a special case of alert based on significant imminence and impact)
  - Alerts: information reflecting periods of increased threats that lack specificity in time or affected entities
  - Guidance: information reflecting best practices in prevention and/or remediation
  - All the while ensuring that the national cybersecurity alert system remains connected and is wholly aligned to the National Cyber Incident Response Plan as it is built out from the extant ad hoc warning system.
- The CISA Director should task the CISA General Counsel (with assistance of the Office of the National Cyber Director chaired cyber lawyers council) to examine and recommend a legal framework, incentives, and protections connected to sharing and acting on cyber threat information.

Conclusion:

There is strong value of a national cybersecurity alert system led by CISA which would leverage and connect the work currently done by various federal agencies, departments and private sector entities. A national cybersecurity alert system should complement rather than replace the continuous exchange of information on cyber risk trends and best practices.

The prospective national cybersecurity alert system should provide specific, actionable and time sensitive information to cyber defenders on imminent cyber risk. As described in further detail in this report, CISA should build on CIRCIA implementation to harness the prospective collaboration between federal agencies to meld CIRCIA information with other streams of threat and vulnerability information. This would feed an alert system led and executed by CISA and relevant agencies possessing unique capabilities and relationships.

Appendices:

Appendix 1: Methodology employed to conduct the national cybersecurity alert system Study

Appendix 2: List of contributors to this report

Appendix 3: Summary notes of subcommittee engagement with Israel Cyber Directorate

Appendix 4: Summary notes of subcommittee engagement with UK National Cyber Security Centre

Appendix 5: Summary of comments and recommendations from the Ploessel CISO engagement

Appendix 6: Overview of U.S. Government Primary Cyber Alerts and Advisories

Appendix 7: Possible Framework for Cybersecurity Information by Type and Level

Appendix 8: Parallels and Differences Between a prospective national cybersecurity alert system and the extant US National Weather Alert System

Appendix 9: Parallels and Differences between a prospective national cybersecurity alert system and the extant US Cyber Terrorist Alert System

Appendix 10: Additional Resources

Appendix 1: Methodology employed to conduct the national cybersecurity alert system study

CSAC established a subcommittee to undertake a broad engagement and iterative development of findings and recommendations that included outreach to the private sector, international counterparts, and federal agencies and departments involved in the assimilation and dissemination of [ad hoc] cybersecurity alerts.

External Outreach (across the period late 2022 to August 2023):

- DHS/CISA to provide specific scenarios that give shape and form of what CISA is looking for
- Explored lessons from the U.S. Terrorism Alert System; and National Weather System (e.g., Hurricane Alerts)
- UK National Cyber Security Center and former senior leaders (Ciaran Martin, Paul Chichester, David Omand)
- Israel National Cyber Center (Gaby Portnoy, Aviram Atzaba, and staff)
- US Office of the National Cyber Director (Brian Scott)
- US Federal CISO and CIO (Chris DeRusha, Clare Martorano)
- The National Security Agency Cyber Security Directorate (Morgan Adamski)
- FBI Assistant Director for Cyber (Bryan Vorndran)
- Canadian Security Establishment (Shelly Bruce; Rajiv Gupta)
- US government cyber lawyers group to explore liability shield or safe harbor for good faith efforts based on warning (Paul Tiao)

Appendix 2: List of contributors to this report

The following NCAS subcommittee members participated in the study and recommendations documented in this report

Subcommittee Members:

- Chris Inglis, Subcommittee Chair, Former National Cyber Director
- Jennifer Buckner, Mastercard
- Kathryn Condello, Lumen Technologies
- Niloofar Razi Howe, Tenable
- Kevin Mandia, Mandiant
- Jeff Moss, DEF CON Communications
- Suzanne Spaulding, Center for Strategic and International Studies
- Alex Stamos, Krebs Stamos Group
- Patrick Turchick, Johnson & Johnson

Interviews were conducted with:

- Israel Cyber Security Center
- United Kingdom National Cyber Security Centre (NCSC)
- Ad hoc group of private sector CISOs facilitated by JCDC participant, Matt Ploessel
- The Office of the National Cyber Director
- The FBI Assistant Deputy Director for Cyber (Bryan Vorndran)

Appendix 3: Summary notes from Interview with Israel's Cyber Directorate, 20 July 2023

Questions teed up by the US NCAS subcommittee to frame the discussion:

- What should a cybersecurity alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to cyber threats?
- What criteria or situations should be considered for such a system, to include risk?
- How would the effectiveness of this new capability be measured?
- Is there a platform or mechanism that would ensure there is widespread awareness regarding this new capability, to ensure it is effectively leveraged?
- What are some lessons learned from other, non-cyber national alert systems?

Israeli team Comments:

- Israel has had an alert system for several years and is currently revamping it based on accumulated experience.
- The system has often been overwhelmed with too many alerts that are poorly distinguished from one another and lack operational context.
- Solution:
  - Prioritization based on the criticality of the impact of a given threat;
  - Crisper role assignment to central and distributed government authorities;
  - Stronger integration of process and operations.
- The Israeli system provides 3 kinds of alerts:
  - Critical function alerts to internal Israeli entities;
  - Alerts (and guidance/assistance) to private sector entities provided by sector leads;
  - Alerts to international partners.
- Alerts should be: actionable; convenient to receive and clear in their meaning;
  - Emphasis: Actionable information is vital.
- Coherence across the multiple participants in an *alert* system is vital (for Israel, the central authority is equivalent to CISA; sector agencies are equivalent to US counterparts; the private sector collaborates more closely with both).
  - The central authority focuses on critical functions (which cut across stove piped sectors) with bias to provision actionable alerts to the most critical functions.
  - Sector agencies focus on their respective sectors with a bias to provision continuous assistance and guidance and provide regulatory oversight.
- Physical integration of the various federal entities participating in this system is important to create the seamless integration of disparity government capabilities, authorities and perspectives.
- One must recognize that the various critical sectors differ significantly in maturity and ability – prioritize your efforts accordingly.

Appendix 4: Summary notes from interview with UK National Cyber Security Centre (NCSC), 1 August 2023

Summary of discussion:

- Inglis led off with a [very] brief summary of the task being worked by the subcommittee and reprised the 4 framing questions sent in advance to the UK discussants:
  - What should a cybersecurity alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to cyber threats?
  - What criteria or situations should be considered for such a system, to include risk?
  - How would the effectiveness of this new capability be measured?
  - Is there a platform or mechanism that would ensure there is widespread awareness regarding this new capability, to ensure it is effectively leveraged?

General [opening] remarks by UK colleagues:

- UK does not have a threat alert system per se; though they have issued NCSC notifications for "heightened threat" (e.g., on the eve of the Russo-Ukraine war) and recommendations for increased preparation during special events (e.g., the London Olympics, coronation, etc.).
- There has been interest in a terrorism-like alert system with a graded scale.
- The challenge is that the terrorism alert system comes with legal and operational implications for each level which are difficult to define for cyber.
- The challenge for cyber is attaching objective legal and action-oriented measures to each of the prospective levels we might employ in such a scheme.
- As a consequence, the UK system is not threat led; (e.g., No shields up) but they do "put a general awareness and preparation wrapper around specific real-world events" (Coronation, Olympics, etc.).
- UK occasionally put out episodic alerts and advisories for specific clusters of providers, operators, and/or sectors. Often based on specific, classified, information. These ad hoc alerts are supported by a monthly session among government representatives of the various sectors served by HMG who, in turn, remain in continuous contact with their private sector counterparts …. The point here is that there is a continuous flow of information, vice episodic threat alerts.
- KEY POINT: UK system is anticipatory and continuous; Emphasis is on preparation vice reaction as the predominant behavior; the UK finds the U.S. goal for a national cybersecurity alert system appealing but the UK does not have a scheme to introduce it with objective, repeatable standards, legal framing, and attendant actions for each.
- The UK recommends the US speak to the Norwegians who have a system called "Cyber Pulse" that seems to capture much of what the US is seeking to install.

US Participant Questions and Comments

- Comment: "Where we [the US and UK combined] are, is not bad … the example of the terrorism alert system is far less helpful than we originally imagined it might be (it is unduly reactive, episodic and focused on the negatives of threat vice the positives of resilience borne of preparation and continuous consultation that addresses and precludes unnecessary risk)".
  - Both countries issue advisories and alerts when we discover a threat (often based on recently discovered technology flaws or a significant rise in threat actor action).
  - The biggest challenge is how you ratchet back down – avoiding the desire to capture the nuance of the situation with a color or a phrase (intuitively appealing though far less useful in practical application).

- Comment: "Preparation seems to be the preferred behavior, vice response".

- Question: "Which messaging is more impactful?"
  - UK response: Specificity is the key – describing the nature of the threat and what the impact would be if

it lands; very important to be specific in describing the nature of the problem and whatever actions may be appropriate to deal with it.

- The discussion concluded at the end of the prescribed 30 minutes allocated. The UK discussants will pass contact information for the Norwegians (their *cyber pulse* system) and any additional comments they may have on the questions posed by US discussants.

Appendix 5: Summary notes from engagement of Private Sector CISO Council

The following was obtained in various conversations with representative – but not exhaustively so – CISOs and JCDC Participants

In general, the private sector seeks greater action ability in disseminated information; greater proactivity in government actions to mobilize disparate authorities to crowd source and interdict cyber threats; and greater coherence in roles and responsibilities of government entities that provide alerts and guidance. *(Detailed, informal, recommendations are under development and can be provided at a later date)*

Specific private sector comments from enterprise security professionals relevant to the creation of a national cybersecurity alert system *are:*

- The alert system should serve ONLY for the timely dissemination of urgent and actionable alerts that enable recipients to anticipate and prepare for specific cyber threats.
- The alerting system should optimize the alerting process and follow on actions to notable cyber incidents that are ongoing or have recently happened and continue to produce damage, vulnerability, and potential harm.
- Optimize the reporting pipeline to incentivize and accommodate high-fidelity, high-value cyber incident reporting sources. Remove friction and promote favorable outcomes. More specifically:
- Emphasize creating mechanism for:
    - Directly reporting to victims or their security vendors that can take actions.
    - Determining relevant **actioning stakeholders** (organizations or people that can take actions to mitigate harm or categorically disable attacker capabilities).
    - Inform the security practitioners at relevant verticals or affected organizations.
    - Use global broadcasting ability ONLY when absolutely necessary.
    - Define a clear value adding function that naturally incentivizes operators to involve CISA in order to reach a favorable outcome.
    - While alerts are inherently and intuitively valuable, the focus must be to enable action that prevents, interdicts and/or disrupts threats.
    - The US government has a unique opportunity to synthesize and disseminate threat information that enables disruption of active threats.

Appendix 6: Overview of U.S. Government Primary Cyber Alerts and Advisories

Background: The complex information sharing and stakeholder relationships among federal agencies have resulted in redundancies and gaps in the presentation and availability of useful cybersecurity products. This section aims to list and describe key products produced by key federal agencies.

Cybersecurity and Infrastructure Security Agency (CISA): CISA leads the nation's efforts to protect and strengthen critical infrastructure against cyber threats. Their focus is on risk assessment, incident response, and information sharing. The following are some of their key cyber alert and advisory products:

- **Security Bulletins:** Comprehensive analyses of emerging threats, trends, and best practices for cybersecurity professionals.
- **Alerts:** Timely notifications addressing significant cyber threats, vulnerabilities, and incidents.
- **Cybersecurity Advisories:** Detailed guidance and recommended actions to mitigate specific cyber risks and vulnerabilities.

Federal Bureau of Investigation (FBI): The FBI plays a crucial role in investigating and combating cyber threats. More specifically, the FBI's role under PPD41 identifies them as a key partner in ensuring that alerts are fully leveraged to enable threat response. Their approach includes proactive intelligence gathering and collaboration with law enforcement agencies. The following are some of their key cyber alert and advisory products:

- **Flash Alerts:** Immediate notifications providing time-sensitive information on significant cyber threats and recommended actions.
- **Private Industry Notifications:** Targeted alerts and information sharing with private sector partners to address emerging cyber threats.
- **Threat Intelligence Bulletins:** Timely bulletins providing insights into emerging cyber threats and recommended actions.
- **Public Service Announcements (PSAs):** Publicly available announcements highlighting significant cyber threats and providing mitigation strategies.
- **Security Advisories:** Detailed advisories on specific vulnerabilities or threats, including mitigation recommendations.

National Security Agency (NSA): The NSA plays a vital role in the nation's cybersecurity by providing intelligence and expertise to protect national security systems. Their products emphasize advanced techniques and insights. The following are some of their key cyber alert and advisory products:

- **Cybersecurity Information Sheets (CSIS):** Brief, practical guidance on critical cybersecurity topics and emerging threats.
- **Cybersecurity Technical Reports:** In-depth reports providing analysis, insights, and technical details on advanced cyber threats and vulnerabilities.
- **Cybersecurity Advisories:** Actionable advisories offering guidance and recommended countermeasures for emerging cyber risks and trends.
- NSA's role as both a source of cyber threat information and as the administrator of the U.S. Intelligence Community's CRITIC alert system (defined under the U.S. Intelligence Community Directive 190), identifies them as a key partner as well.

Appendix 7: Possible Framework for Cybersecurity Information by Type and Level

	Threat	Vulnerability	Dependency
Strategic *Long-term data and analysis that captures, assesses, and forecasts trends, directly informing an organization's year-over-year cybersecurity planning, budget allocation, and decision-making.* *It serves to establish the* ***baseline*** *of the cyber environment.*	Characterization and assessment of threat actor's objectives, constraints, and targeting preferences Trends and evolution of threat actor tactics, techniques, and procedures Assessment and forecast of behavioral or operational change based on external factors (geopolitical, economic, etc.).	Assessment of common or emerging methods of exploitation and intrusion Reports on emerging technology weaknesses Evaluation of procedural weaknesses against best practices	Assessment of trends in trade and supply-chain dependency. Assessment of market consolidation, acquisition, or other factors that shift centralization of risk Assessments or identification of cross-sector dependencies Assessment of common technology products or services shared among enterprises
Operational *Data and information from routine assessments, ad hoc reporting, and forecasts or assessments that report deviations from baseline to address cybersecurity issues in day-to-day operations.*	Updates to cyber threat actor behavior and tactics Identification and disclosure of on-going campaigns Monitoring of deep and dark web hacking forums Assessment of shifts in geopolitical factors (tension, conflict)	Risk and vulnerability assessments External audit or remote vulnerability scanning Red-teaming and penetration testing Notice of deprecation of support to product	Monitoring third-party security (External audits of critical vendors) Risk assessments for key dependencies (Industry or government reports) External dependency assessments
Tactical *Encompasses information that is intended to inform or prompt immediate action, often with the aim of discovering, preventing, or mitigating a near-term harm.*	Published or shared Indicators of compromise Victim notification of compromise News reporting	Notifications of newly-discovered vulnerabilities. Immediate patching and mitigation (vendor remote update) Notification of vulnerability (CISA scan)	Notice of planned outage (vendor or government communication) Vendor disclosure of compromise or incident

Appendix 8: Parallels and Differences Between a prospective national cybersecurity alert system and the U.S. National Weather Alert System

Similarities:

- Addresses a hazard shared by 'many' (weather or cyber threat)
- Establishes efficient and effective mechanisms for collection and dissemination of hazard information from party(ies) to affected parties
- General information about strategic weather patterns Is differentiated from specific tactical warning
- Has both push and pull modalities

Differences:

- Weather does not adjust to changes in its victims' disposition or awareness; Cyber threat actors do
- Weather holds all in its path at common risk (broadcast modes appropriate); Cyber is often more selective (selective dissemination)

Appendix 9: Parallels and Differences between a prospective national cybersecurity alert system and the National Terrorism Advisory System

Similarities:

- Addresses a hazard shared by 'many' (e.g., terrorism by one, cyber threat by the other)
- Both systems aim to create efficient and effective mechanisms for collection and dissemination of hazard information from party(ies) to affected parties
- Warnings may be either general or specific - General information about strategic threat level is differentiated from specific, imminent, and tactical warning (the latter is preferred)
- The threat can/does react and change based on the awareness and preparation of intended victims

Differences:

- Most of the tools to prepare, mitigate threat, and defend from fist response through recovery are in the private sector (in the GWOT, the government was the principal actor for counterterrorism; Notifications were largely intended to reduce the attack surface in/of private citizens and their materiel. In cyber, a warning may be intended to stimulate a defensive action by a private sector entity whose actions then mitigate threat and/or extend protections to others).

Appendix 10: Additional Resources

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

CISA National Cyber Incident Scoring System (NCISS), September 30, 2020

https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

Presidential Policy Directive – United States Cyber Incident Coordination, July 26, 2016

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

CISA Stakeholder-Specific Vulnerability Categorization (SSVC)

https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

U.S. Intelligence Community Critical Information (CRITIC) Program

https://www.dni.gov/files/documents/ICD/ICD%20190.pdf

Homeland Security Advisory Council, Homeland Security Advisory System Task Force Report and Recommendations, September 2009

https://www.dhs.gov/xlibrary/assets/hsac_task_force_report_09.pdf

DRAFT REPORT TO THE CISA DIRECTOR

Building Resilience and Reducing Systemic Risk to Critical Infrastructure

September 13, 2023

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established a Building Resilience and Reducing Systemic Risk to Critical Infrastructure (SR) subcommittee (hereinafter referred to as the "Subcommittee") to enhance national resiliency.

Previous recommendations were organized around three pillars:

I. Analyze systemic risk to identify systemically important entities.
II. Establish national resiliency goals to drive common analysis and action.
III. Create or enhance enabling structures and programs to advance national resiliency.

In a formal response letter from CISA Director Easterly to the CSAC on March 1, 2023, Director Easterly stated recommendations (in support of the three pillars) were either "Accepted" or "Partially Accepted." These recommendations are fundamental and foundational to the collective capability of each sector to support national risk efforts.

In March 2023, CISA provided a new tasking document to the CSAC, outlining three areas of study. The CISA National Risk Management Center (NRMC) is interested in reducing risk to critical infrastructure and measuring the efficacy of their role in doing so. The Subcommittee was tasked to provide a critical infrastructure perspective to inform these efforts.

The Subcommittee tasking document also included the following tasking questions to guide the Subcommittee's work:

1. How can the governance, processes, and analysis in CISA's National Critical Infrastructure Risk Register create the greatest opportunity for risk reduction?
2. What risk information would help private sector entities, especially systemically important entities (SIEs), plan and execute risk reduction measures?
3. How can CISA incentivize close collaboration between SIEs and the U.S. government on their security and resilience?

Findings

The Subcommittee members conducted a series of meetings to ensure that CISA's Joint Cyber Defense Collaborative (JCDC), National Risk Management Center (NRMC), and Stakeholder Engagement Division (SED) are aligned on work concerning critical infrastructure. Special topical meetings included NRMC's SIE criteria and methodology, the SED's SIE Outreach Initiative, and evaluation of Space as an independent sector.

The Subcommittee members agreed that its work would focus on architecture and capabilities to optimize collaboration between the critical infrastructure and the U.S federal government, as well as a reimagination of the public-private partnership for national security, risk, response, and resilience.

To understand the current landscape of operational collaboration, the Subcommittee members conducted a series of sector-specific engagements across seven sectors/subsectors.

1. Energy (electricity, oil and natural gas, dams, nuclear)
2. Finance
3. Communications
4. Transportation (railways, airlines, shipping, trucking)
5. Healthcare
6. Water
7. Chemical

The goal of these engagements was to solicit feedback on how the federal government—especially, but not exclusively, CISA's NRMC, SED, and JCDC—can most effectively collaborate on national security, critical infrastructure protection, and risk management issues with critical infrastructure owners and operators, associated vendors, and other stakeholders. The engagements addressed the following topics:

- The appropriate mix of stakeholders with which the federal government can engage when seeking private sector input on national security, critical infrastructure protection, and risk management activities and policies (e.g., Sector Coordinating Councils, Information Sharing and Analysis Centers, Section 9-designated entities, state and local government entities and international partners);

- The venues and mechanisms through which the federal government should engage such stakeholders (e.g., the role of Sector Risk Management Agencies (SRMAs), the NRMC, SED SIE Outreach Initiative, JCDC, and other government-, industry- and public-private bodies); and

- Strategic and long-term goals for federal government consultation with critical infrastructure owners and operators (e.g., how industry-specific mechanisms and exchanges can be leveraged to provide sustained support for such efforts, integration with other elements of government, such as intelligence and law enforcement entities, and how to facilitate cross-sector engagement in such efforts).

The Subcommittee members considered what attributes a sector (or other organizing function) might require for effective operational collaboration. In developing the attributes for architecture for operational collaboration, they referenced the New York Cyber Task Force's definition of Operational Collaboration as, "the integrated public-private preparation and response to severe cyber crises"[1]:

In response to the Subcommittee's taskings regarding the optimization of governance, processes, and analysis within CISA's National Critical Infrastructure Risk Register, comprehensive insights are provided. These insights are aimed at fostering risk reduction, enhancing collaboration, and establishing a robust feedback loop/cycle with the private sector, particularly SIEs, to build a more resilient critical infrastructure landscape.

There are three critical attributes for the architecture of a sector's operational collaboration model.

1. Risk Analysis and Mitigation - Enables a deeper understanding of how systemically important functions (i.e., National Critical Functions (NCFs)) operate, including business and technical underpinnings, as well as national security impact of compromise.

2. Illumination of the Battlefield - Drives a risk-informed intelligence collection and analysis apparatus that integrates the capabilities and accesses of private sector and government organizations. Provides early warning capability of

[1] https://www.sipa.columbia.edu/sites/default/files/2023-02/NYCTF%202020%20Operational%20Collaboration-report.PDF

adversary intent/capability.

3. Integrated Response - Enables government and critical infrastructure to respond to an event by collaborating and sharing information about attacks and risk mitigating actions to change the trajectory of our country's and industry's collective defense, response, and resilience.

The tactical elements that can produce an effective architecture and capabilities include:

- Government and private sector convening structures that are integrated and enable collaboration among different peer groups (i.e., CEO, CIO, CISO, COO, operations, risk management, incident response, etc.). Use of existing convening structure that is CEO-connected at minimum, if not led (Sector Coordinating Councils (SCCs), Information Sharing and Analysis Centers (ISAC), Section 9, the President's National Security Telecommunications Advisory Committee (NSTAC), etc.);
- Integration of steady state policy coordinating bodies with purpose-built incident response entities.
- Section 9 and/or SIE–specific organizations that are integrated with broad-based sector-wide collaboration centers.
- Clear collaboration and throughput between:
    - Private sector: owners/operators (i.e., firms), industry associations, collaboration centers (e.g.., ISAC, Analysis and Resilience Center for Systemic Risk (ARC), Department of Energy's Energy Threat Analysis Center (ETAC) etc.), and SCCs
    - Government: Department of Defense, law enforcement, Intelligence Community (IC), CISA/DHS, SRMAs, Government Coordinating Councils (GCC)
- Focus of the convened group should be consistent with national security objectives (e.g., for alignment with CISA's NRMC and JCDC, and FEMA) and address the following questions:
    - Is there credibility with SRMAs; is the appropriate level at table from Federal government? (Example Deputy Secretary or higher)
    - Is convening structure sustainable and adaptable;
    - Able to avoid duplication or pancaking layers of regulation;
    - Able to assess interdependencies and 1st, 2nd, 3rd derivative issues, including supply chain;
    - Able to integrate with:
        - SRMA
        - IC; FBI, US Cyber Command, Secret Service, National Security Agency, Office of the Director of National Intelligence
        - Department of Defense, Federal Bureau of Investigation, Secret Service
        - Other private sector critical infrastructure participants/interdependencies
        - State, Local, Tribal, Territory (SLTT)
        - International

Recommendations

- With respect to recommendations identified in September 2022, implementation of recommendations is underway and should be consistent with outcome of the PPD-21 Rewrite. CISA should not proceed with SIE designations until it collaborates with private sector regarding existing critical infrastructure designations and authorities (i.e., EO 13636 Section 9).

- CISA should develop an ongoing process for reviewing attributes and maturity model for achieving operational collaboration. The process should be managed by CISA with sector-led implementations conducted by SRMAs/GCCs and SCCs. This maturity model would create a pathway for both industry and government capabilities to progress in an organized and coordinated fashion that is accountable to scrutiny.

- CISA should more clearly define their role as National Coordinator with supporting architecture and an organizational structure. This structure should include defined SRMA roles, responsibilities, and capabilities. At a minimum, CISA should ensure sector-specific points of contacts for ease of integration by non-CISA personnel (SRMAs and Sectors/Subsectors).
    - This recommendation also supports the White House National Cybersecurity Strategy implementation plan 1.2.5 tasking of "Establish an SRMA Capability".
    - See Appendix A SRMA ANNEX as a template example.

- CISA, as the lead agency responsible for the White House National Cybersecurity Strategy implementation plan 1.4.1 tasking "Update National Cyber Incident Response Plan" (NCIRP), should develop an owner/operator-centric update to the NCIRP. Rather than considering what government needs to support its decision making and efforts, it should use a first-principles approach to considering how the government can support owners/operators during crisis.
    - The NCIRP update should also align to FEMA's incident response plan. CISA should include the critical infrastructure asset owners and operators as part of the tasking team.

- The National Critical Infrastructure Risk Register exemplifies CISA's commitment to bolstering our national security. To maximize the potential for risk reduction, CISA must refine the governance structure to encompass designated critical infrastructure private sector representatives. CISA should establish dedicated working groups—where public and private experts collaboratively engage in risk analysis—to ensure comprehensive insights that effectively mirror real-world scenarios. Additionally, recognizing the pivotal role of SCCs, CISA should encourage these councils to integrate experts to address intricate risk scenarios in support of a national risk strategy.

- To the extent that sectors/subsectors have already developed a risk register, CISA and SRMAs should align their own efforts with industry approaches where possible and appropriate.

- CISA's collaboration with SRMAs has proven instrumental but needs improvement. To operationalize the aggregate efforts and effectively diminish risk, CISA's NRMC should engage in regular collaboration with the critical infrastructure private sector. This engagement should extend to promote systemic interaction with CISA's JCDC, the SCCs, GCCs, and SRMAs—ensuring all stakeholders with relevant expertise are at the decision-making table and have common operating picture across sectors. This recommendation is stated without insights from the SIE beta list or the National Critical Infrastructure Risk Register currently under development at CISA. These were never shared with the Subcommittee.

- Architecture from both the private and public sector for operational collaboration will form a sustaining approach. CISA should explore ways to establish a standing, private sector CEO-led Committee that would report directly to the President of the United States, with participation from the Office of National Cyber Director, National Security Council, CISA Director and the Homeland Security Advisor, to ensure that resilience—including continuity planning-- is a priority. The function of this Committee would be to support the Continuity of the Economy through exercises with Cabinet-level members.

Conclusion

Consistent with Cyberspace Solarium Commission recommendations, the heart of this work has been to operationalize the proposed collaboration between the private sector and the federal government. The recommendations provided above seek to illustrate this constructive collaboration. Much work is underway and should be noted that this needs to be an evergreen evaluation.

Appendix A: List of Contributors to this Report

The following SR subcommittee members participated in the study and recommendations documented in this report.

Tom Fanning, Subcommittee Chair, Southern Company
Marene Allison, Former Johnson & Johnson
Lori Beer, JPMorgan Chase
Rahul Jalali, Union Pacific
Jim Langevin, Former U.S. House of Representatives
Cathy Lanier, National Football League
Kevin Mandia, Mandiant
Suzanne Spaulding, Center for Strategic and International Studies
Alicia Tate-Nadeau, Illinois Emergency Management Agency

APPENDIX B **Sector Risk Management Agency (SRMA) Energy Annex (Recommendation 3 template example)**

Sector Risk Management Agency:	Support Agencies:
Department of Energy	Department of Homeland Security Department of Transportation Department of Defense Department of Justice Office of the Director of National Intelligence Office of the National Cyber Director Federal Energy Regulatory Commission

INTRODUCTION

Purpose

[same across SRMAs – outlines purpose of SRMAs generally and the purpose of each annex]

Scope

The term "energy" includes producing, storing, refining, transporting, generating, transmitting, conserving, building, distributing, maintaining, and controlling energy systems and system components. The sector includes the electricity, oil, and natural gas subsectors but excludes the hydroelectric and commercial nuclear power facilities and pipelines. [additional information defining the scope of the sector]

CROSS-SECTOR DEPENDENCIES

This section describes how the energy sector supports and relies on other critical infrastructure sectors.

Transportation Systems Sector

The energy sector's heavy reliance on pipelines to distribute products across the nation highlights the interdependencies between the energy and transportation systems sectors. The transportation systems sector is also designated a lifeline function, meaning its reliable operation is so critical that a disruption or loss of function will directly affect the security and resilience of other critical infrastructure sectors, including energy. The dependencies are reciprocal: the transportation systems sector is dependent on the energy sector for fuel to operate transport vehicles and power for overhead transit lines. Within the energy sector, transportation electrification is shifting the dependency away from the oil and natural gas subsector toward the electricity subsector.

Communications Sector

Both the energy sector and the communications sector provide lifeline functions, meaning they are highly interdependent. The communications sector relies on the energy sector for fuel to maintain temperatures for equipment and to provide backup power and energy to run cell towers and other transmission equipment. In turn, the energy sector is dependent on the communications sector to perform many monitoring and control functions, including breakage and leak detection and remote control of operations on the oil and natural gas side and the detection and maintenance of operations and electric transmission on the electricity side.

Water Sector

The energy sector's reliance on water stems from the importance of water in production operations for both the electricity and natural gas subsectors and the use of water as a coolant in many power generation facilities. Water treatment plans rely on the energy sector for fuel and electric power to operate pumps and treatment plants.

Information Technology Sector

Increasing cyber and information technology dependencies have created new and evolving risks for the energy sector.

Energy control systems and the information and communications technologies on which they rely play a key role in North American energy infrastructure. These cyber and information technology components are essential in monitoring and controlling the production and distribution of energy.

Critical Manufacturing Sector

Concerns about the availability and security of critical energy sector goods and components sourced from adversary nations have exacerbated supply chain constraints facing the energy sector. The energy sector relies heavily on the domestic critical manufacturing sector to provide materials like large power transformers, semiconductors, solar photovoltaics, and other key inputs to energy systems and processes. Long lead times for key operational equipment can create reliability and security concerns for the sector by stressing the ability of critical infrastructure owners and operators to respond to natural disasters and man-made threats.

Other Sectors and Dependencies

Given that energy infrastructure provides essential fuel and power and provides one of the four lifeline functions, all other critical infrastructure sectors experience interdependency with the energy sector. Shared dependencies on the providers of the other three lifeline functions also create risks for the energy sector. Geographic co-location can also create interdependencies between critical infrastructure owners and operators, and sector risk management agencies should account for the geographic placement of critical infrastructure facilities when scoping cross-sector risk management activities. In addition to cross-sector dependencies, the energy sector is characterized by dependencies between the natural gas and electricity subsectors. Natural gas is used for electric generation, yet constrained infrastructure to deliver natural gas supplies to power generators in certain locations create reliability issues. The natural gas subsector also depends on electricity at production, pipeline, processing, and distribution facilities.

CORE CAPABILITIES AND ACTIONS

As described in Presidential Policy Directive 21 and U.S. Code at 6 U.S.C. § 665d, national infrastructure security is built on a partnership between government and private industry that combines the implementation of policy, regulatory, and voluntary actions to manage risk. Both public and private entities own and operate the nation's critical infrastructure, but the risk associated with the destruction or failure of that infrastructure is borne by a much larger population of Americans—and disproportionately by vulnerable or disadvantaged communities and people of color. For this reason, the effort to secure the nation's critical infrastructure requires a whole-of-government approach and coordination and collaboration across multiple intergovernmental and industry stakeholders. This section outlines the core capabilities, as identified by the CISA's list of National Critical Functions, that the energy sector supports and specifies the responsibilities of the sector risk management agency and each supporting agency.

Energy Sector Alignment with National Critical Functions

National Critical Function	Energy Sector
Generate electricity	
Transmit electricity	
Distribute electricity	
Exploration and extraction of fuels	
Fuel refining and processing fuels	
Store fuel and maintain reserves	
Provide material and operational support to defense	
Provide and maintain infrastructure	

Agency Functions

Sector Risk Management Agency	Functions
Department of Energy (DOE)	**Support sector risk management** • Establish and carry out programs to assist critical infrastructure owners and operators within the energy sector and its subsectors in identifying, understanding, and mitigating threats, vulnerabilities, and risks to energy systems or assets. • Recommend security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets. **Assess sector risk** • Identify, assess, and prioritize risks within the energy sector and its subsectors, considering physical security and cybersecurity threats, vulnerabilities, and consequences. • Support national risk assessment efforts led by the Department of Homeland Security. • Participate in planning efforts related to the revision of the *National Infrastructure Protection Plan* and the development and revision of the energy sector-specific plan.

	Sector coordination • Serve as day-to-day federal interface for the prioritization and coordination of sector-specific activities and responsibilities. • Serve as the federal GCC for the energy sector and facilitate interagency, intergovernmental, and cross-jurisdictional coordination on issues affecting the energy sector as they pertain to critical infrastructure security and resilience. • Participate in cross-sector coordinating councils, including the Federal Senior Leadership Council. **Facilitate information-sharing** • Facilitate access to and exchange of information and intelligence necessary to strengthen the security of energy sector critical infrastructure, including through the Electricity-ISAC and the ETAC. • Facilitate the identification of intelligence needs and priorities of energy sector critical infrastructure owners and operators in coordination with the Director of National Intelligence. • Support DHS reporting requirements by providing energy sector-specific critical infrastructure information. **Support incident management** • Support incident management and restoration efforts during or following a security incident. • Support the CISA Director in national cybersecurity asset response activities for critical infrastructure. **Contribute to emergency preparedness efforts** • Coordinate with energy sector owners and operators and the CISA Director in the development of planning documents for coordinated action in the event of a natural disaster, act or terrorism, or other man-made disaster or emergency. • Participate in, conduct, or facilitate exercise and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the energy sector. • Support the Department of Homeland Security and other federal departments and agencies in developing planning documents or conducting exercise or simulations when relevant.

Support Agency	Functions
Department of Homeland Security (DHS)	**Cybersecurity and Infrastructure Security Agency** • Execute roles and responsibilities—including partnership management; planning, analysis, and reporting; capacity building; information sharing; and incident management—as National Coordinator through the Federal Senior Leadership Council. (per the 9002 (b) report) • Ensure a unified approach to risk management across critical infrastructure sectors. • Facilitate the development of standardized methodologies for assessing the maturity and effectiveness of sector-specific partnership structures. • Maintain and periodically facilitate a process for updating the sector-specific annexes outlining SRMA roles and responsibilities. • Maintain the National Coordinator assistance model to outline the provision of CISA resources to SRMAs for enhanced coordination and technical support for sector-level risk analysis. • Receive and analyze sector-specific information provided annually by SRMAs to identify opportunities for cross-sector collaboration on risk management activities. • Work with the Office of the National Cyber Director to engage the Office of Management and Budget to identify budgetary requirements for energy sector risk management activities. • Operate the Joint Cyber Defense Collaborative and coordinate energy sector-specific operational collaboration activities with the Energy Threat Analysis Center. **Transportation Security Administration** • Support risk assessment and management activities as they relate to pipelines serving energy infrastructure. **Federal Emergency Management Agency** • Provide oversight of emergency preparedness activities carried out under ESF #12. • Maintain the National Response Framework or its successor as the organizing concept for emergency preparedness and disaster response efforts.
Department of Transportation (DOT)	**Pipelines and Hazardous Materials Safety Administration** • Support risk assessment and management activities as they relate to pipelines serving oil, natural gas, and other energy infrastructure. • Develop and implement safety regulations and guidance for pipelines, underground natural gas storage, and liquified natural gas facilities.
Department of Defense (DOD)	• Operate, defend, and ensure the resilience of all DOD-owned or contracted critical infrastructure. • Secure national security and military systems. • Investigate criminal cyber activity under military jurisdiction.

Department of Justice (DOJ)	Federal Bureau of Investigation • Lead counterterrorism and counterintelligence investigations and related law enforcement activities. • Conduct domestic collection, analysis, and dissemination of cyber threat information. • Operate the National Cyber Investigative Joint Task Force.
Office of the Director of National Intelligence (ODNI)	• Use applicable authorities and coordination mechanisms to provide intelligence assessments regarding threats to critical infrastructure and coordinate intelligence and other sensitive or proprietary information related to critical infrastructure. • Oversee information security policies, directive, standards, and guidelines for safeguarding national security systems.
Office of the National Cyber Director (ONCD)	• Work with the Cybersecurity and Infrastructure Security Agency to engage the Office of Management and Budget to identify budgetary requirements for energy sector risk management activities.
Federal Energy Regulatory Commission (FERC)	• Facilitate the exchange of information with critical infrastructure owners and operators during incident response and recovery. • Encourage critical infrastructure owners and operators to participate in public-private partnerships. • Ensure sector resilience through policymaking and oversight.

Other Stakeholder Functions

Stakeholder	Functions
Systemically Important Entities	• Participate in national risk management activities through the Electricity Subsector Coordinating Council and/or the Oil and Natural Gas Subsector Coordinating Council. • Undertake internal activities and engage in sector and cross-sector activities to conduct risk assessments, understand dependencies and interdependencies, develop and coordinate emergency response plans, establish continuity plans and programs, participate in training, and exercise activities, and contribute technical expertise to critical infrastructure security and resilience efforts. • Adhere to industry best practices and comply with all applicable laws and regulations regarding security practices.
Electricity Subsector Coordinating Council	• Serve as the electricity subsector policy coordination and planning entity to collaborate with DOE as the SRMA and chair of the GCC. • Represent principal entry point for the government to collaborate with the electricity subsector for critical infrastructure security and resilience activities. • Serve as a strategic communication and coordination mechanism between owners, operators, suppliers, and, as appropriate, the government during emerging threats or response and recovery operations. • Participate in planning efforts related to the revision of the *National Infrastructure Protection Plan* and the development and revision of the energy sector-specific plan. • Review the annual submission to DHS on electricity subsector activities. • Understand and communicate requirements of the subsector for government support. • Provide input to the government on research and development efforts and requirements for the electricity subsector.

Oil and Natural Gas Subsector Coordinating Council	• Serve as the oil and natural gas subsector policy coordination and planning entity to collaborate with DOE as the SRMA and chair of the GCC. • Represent principal entry point for the government to collaborate with the oil and natural gas subsector for critical infrastructure security and resilience activities. • Serve as a strategic communication and coordination mechanism between owners, operators, suppliers, and, as appropriate, the government during emerging threats or response and recovery operations. • Participate in planning efforts related to the revision of the *National Infrastructure Protection Plan* and the development and revision of the energy sector-specific plan. • Review the annual submission to DHS on oil and natural gas subsector activities. • Understand and communicate requirements of the subsector for government support. • Provide input to the government on research and development efforts and requirements for the oil and natural gas subsector.
Electricity Information Sharing and Analysis Center	• Provide trusted communities and frameworks for critical infrastructure sectors to facilitate the sharing of timely, actionable, and reliable information for situational awareness. • Provide in-depth comprehensive sector threat and incident analysis and enable aggregation and anonymization of data. • Provide all-hazards threat warning and incident reporting to enhance member risk mitigation activities. • Participate in the planning, coordination, and conduct of energy sector exercises.
Energy Threat Analysis Center	• Work with the sector's information sharing and analysis centers and sector owners and operators to conduct advanced analysis of threats and incidents affecting the energy sector. • Enable shoulder-to-shoulder collaboration between the federal government and critical infrastructure owners and operators, including the fusing of information and sharing of analytic tools and capabilities. • Develop targeted guidance for the energy sector based on government-issued threat alerts for dissemination via the sector's information sharing and analysis centers. • Provide support for ESF #12 activities in the event of an incident affecting energy systems.
Federally funded research and development centers	• Leverage analytic tools and processes in support of risk management activities affecting the energy sector. • Support research and development activities aimed at enhancing the security and resilience of energy sector infrastructure.

DRAFT REPORT TO THE CISA DIRECTOR

Technical Advisory Council

High-Risk Community Protection

September 13, 2023

Introduction:

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Technical Advisory Council (TAC) subcommittee with the purpose of researching ways to better inform CISA's efforts with the Joint Cyber Defense Collaborative (JCDC) and its High-Risk Community Protection (HRCP) initiative.

CISA defines High-Risk Communities (HRC) as those which meet all three of the following criteria:

1. Demonstrated history of being targeted by advanced persistent threat (APT) actors.
2. Limited capacity to provide for their own defense.
3. Limited cybersecurity assistance from the United States Government (USG).

Civil society is the first community CISA is prioritizing for the HRCP initiative, but over the coming years CISA plans to expand support to other communities, such as USG employees using non-enterprise devices.

CISA's HRCP initiative, announced at the Summit for Democracy on March 30, 2023, is dedicated to strengthening the cybersecurity of high-risk communities in the United States. To start, this initiative will engage civil society organizations to learn more about the threats they are facing and how to find the support they need. Through the JCDC, CISA will lead planning efforts with key government and non-government organizations, and cybersecurity and technology companies to develop a cyber defense plan for the domestic civil society organizations which are at high-risk of being targeted by foreign state actors, or non-state groups, foreign or domestic that may seek to impede or discredit the work of civil society organizations.

While focused domestically, CISA's HRCP initiative will also contribute to the Strategic Dialogue on Cybersecurity of Civil Society under Threat of Transnational Repression, co-hosted by the United States and the United Kingdom. As part of this Strategic Dialogue, CISA and its counterparts from Australia, Canada, Denmark, Estonia, France, Japan, New Zealand, Norway, and the United Kingdom will work to improve the cybersecurity of civil society organizations, engage in information sharing on the threats facing high-risk communities, and identify opportunities for greater collaboration.

High-risk communities need to defend against common cyber threats like account takeovers, crypto miners, email scams, data leakage, and ransomware. But for organizations at high-risk of being targeted by foreign state actors, threats may also include organized online threats and harassment, espionage, and sophisticated spyware. The broad range of threats, coupled with their limited defensive capabilities, is what makes high-risk communities so vulnerable. Communities that, due to political or technical factors, consider themselves at low risk one day, might suddenly find themselves in a high-risk situation the next. For example, human rights organizations in an evolving conflict zone or a reporter who publishes an unfavorable article about a political party that then gains power.

The CISA *Shields Up: Guidance for Organizations* webpage outlines foundational principles for protecting organizations and is an effective baseline guidance for high-risk organizations. The goal of this document is to provide threat and defensive guidance, assuming these organizations are already following *Shields Up* guidance.

Currently, high-risk communities count on limited support based on the goodwill of a handful of private companies to help with securing cloud-based email accounts, provide distributed denial of service (DDoS) protection for a community's web presence, or the creation of tools to help lock down devices. Different technology companies have different sets of features to increase the level of security of targeted community members, for example, Apple's "lockdown mode" for their iPhones.

These efforts are good for the communities, but a more structured framework is needed to maximize protection at scale. For example, a structure could be coordinated such that companies already offering free services are not overly duplicating efforts and are communicating with each other to better detect threats. CISA could identify gaps and, in coordination with the protection community, could determine how to best fill them.

CISA is positioned at the intersection of high-risk communities, industry, academia, security researchers, and government. This locus grants it a powerful role in clarifying threats. For example, in helping high-risk communities determine their preliminary risk level. It also provides the opportunity to act as a facilitator in connecting these high-risk communities with security organizations and researchers, and vice-versa.

Helping members of a high-risk community to self-assess their risk level is a critical skill, and it can inform the types of protective behaviors necessary to ensure their safety. While there is no industry specific definition of what a "high" risk is, there is some consensus around factors that would constitute a high-risk. For example, a journalist organization that is reporting critically on an undemocratic state actor with a history of using malware on its opponents would be at high-risk, especially if the organization's cyber maturity and computer security resources are low.

Generally speaking, the higher the likelihood that an organization will be targeted the greater their risk. Risk can be reduced through developing and following a security program, such as the CISA *Shields Up* program, that takes into account the threats an organization faces. To illustrate this, consider the following examples of where a community would be at high-risk:

High Threat and Low Defense capacity:

High Threat: Operates in one or more non-democratic regimes, in a manner that can upset existing power structures, and the regime(s) have a history of cyberattacks, malware and harassment campaigns.

Low Defensive Capacity: No internal IT support, outdated equipment, need to use insecure channels to communicate in the country, must operate in a public manner.

An organization may be considered high-risk if they are currently the target of a harassment campaign or work within a political environment, and are underprepared to resist social engineering threats, with an underdeveloped security team that lacks a patching schedule, password management strategy, and multifactor authentication program.

As another example, if an organization works within a highly competitive environment, it may be considered high-risk because it is more likely to receive targeted spear phishing emails and calls, attempts to harass or discredit executive staff, and solicit company proprietary data with the adversary focusing on exfiltrating and leaking sensitive company data to derail competition.

It might be tempting for an under-resourced organization to decide that it is not at high-risk and therefore not much needs to be done, or to decide that in fact it is at a high-risk and so every security measure must be taken, regardless of effectiveness or cost. Regardless of what is decided, adversaries are constantly adapting and organizations will need to constantly evaluate its responses.

Once an organization has determined its threat and risk level, then it needs to take steps to safely operate at that level. From a technical perspective this could mean configuring its devices and infrastructure to operate at a higher security mode, adopting enhanced email attachment protection, moving functions to the cloud, and so on. Below is an example of the different types of advice which would be given to better protect a given device given a threat level:

Defensive posture for High-Risk Communities generally has four components:

1) Defense at the device level
    - This includes attacks against individual devices with malware, exploitation of OS or applications, and physical attacks to extract data.
2) Defense at the cloud level
    - This includes attacks against user identity such as email phishing or when combined with device attacks that use tokens or credentials to access data stored in the cloud.
3) Defense at the infrastructure or network level
    - his includes lateral movement attacks, unpatched infrastructure, misconfigured infrastructure, poor security posture management, insufficient privilege management and other systemic issues.
4) Minimize human risk
    - This includes attacks against the humans within an organization to gain access to data, money, resources, trust, access and power. Attack vectors typically include email, phone call, text message, social media, and physical threats.

The focus of this report is on technical cyberattacks and does not include threats like in-person attacks or espionage through undercover activities of a nation state. We recognize that these are threats that high-risk communities face; however, they are not explored in detail in this report. CISA can have an important role in protecting communities from offline harms.

Findings:

What communities should CISA support and in what order of priority as we grow into this mission space?

The needs of high-risk civil society vary greatly. Some organizations' primary risks are related to physical safety, intimidation, abuse, outing of members, and social engineering. Others are information related, such as spyware to reveal sources and methods, compromising accounts to impersonate people or the organization, planting false evidence, stealing money or deleting information.

Priority of support within the larger set of civil society communities is subjective; the mission of a community that is critical today may not be so tomorrow.

What is universal is the need for organizations to learn how to self-assess their risk and be able to access the tools, training, and resources to improve their security posture.

Prioritizing which communities to support and in what order requires first an understanding of which communities exist, what their missions are, which risks they face, and how CISA can best support them.

Individuals, such as Lama Fakih, Roman Gressier, and Artemis Seaford, have been targeted by nation-states with sophisticated spyware. See Appendix A for further information on these individuals. Their experiences may help CISA and its partners shape the JCDC HRCP initiative. Furthermore, by facilitating the sharing of these individuals' experiences, both in terms of gaps that led to compromise and steps taken to recover, CISA can demystify the risks and recovery steps for individuals at threat of future or under active attack.

There are numerous entities that act as hubs supporting other smaller entities within a community. For example, Internews, a 501(c)(3) non-profit, "supports independent media in 100 countries," including providing training for journalists and digital rights activists and tackling disinformation. Access Now has a free, 24/7 digital security helpline for members of civil society. The organization has previously collaborated with both Amnesty International and Citizen Lab to investigate attacks leveraging NSO Group's Pegasus spyware.

CISA has an opportunity to engage with a diverse set of high-risk civil society organizations, including ones focused on digital and human rights, reproductive rights, elections, healthcare, and journalism. CISA can better support high-risk organizations by gaining an understanding of what the organization does and how it operates, constraints such as funding, resources, support, threats to the organization and/or staff members, and what are the minimum technology communication requirements when they might need to enter "safe mode."

This type of high-risk support may benefit from a multi-faceted collaboration, including global collaboration with law enforcement and intelligence agencies. These partners can then provide technical examples of how attackers are targeting phones, laptops, social media and email to harm high-risk communities and individuals. It is essential to integrate data about hate crimes, political targeting, and counterintelligence efforts to better inform high-risk communities of what the threats are, how they operate, what to look out for, how to know they being targeted, and whom to call for help.

While the focus of this document is domestic, CISA should recognize that international high-risk communities might be using products and services based in the United States. Providing security guidance to these well-resourced and sophisticated enterprises will help improve high-risk community protection globally.

Within those communities, which type of entities should CISA support and in what order of priority? For example, should CISA focus on individuals, family members, a wide swath of non-profit organizations, or a few key force-multiplier organizations?

Prioritizing non-profit and non-government organizations (NGOs) that are already doing security enhancement work will likely be the most effective way to reach and assist in developing the cybersecurity practices of high-risk communities and the organizations that serve them. Focusing on non-profits and other entities that these communities depend on, especially those that help train and support other communities and act as hubs, will also allow CISA to achieve a greater reach with their resources.

Thus, while it is critical to ultimately help individuals and their family members, direct focus on these groups will not be as effective as working with entities in the space. Moreover, individuals within high-risk communities may be more inclined to trust and use digital security advice provided by NGOs they are already familiar with, and from NGOs who are already attuned to the communities needs and particular circumstances. Given the breadth of needs, some NGOs improving digital security in high-risk communities focus on taking a "train the trainer" approach, that will help scale efforts over a one-by-one approach.

For example, the Security Education Companion is a project to provide articles, lesson plans, and teaching materials for people teaching digital security. It was created by the Electronic Frontier Foundation and is now maintained by the Level Up network and fellow community contributors, coordinated by Simply Secure, and hosted by the EFF. The project includes practitioners from Access Now, Internews, the Library Freedom Institute, and several other organizations. Appendix B lists a set of digitally focused NGOs that will provide a useful starting point for CISA.

This type of effort allows the sophisticated NGOs in the digital security space to help keep advice and training high quality and up to date, while enabling communities with less cyber maturity to learn and then pass on those learnings to their own communities.

While "a journalist targeted by sophisticated spyware" and "healthcare worker targeted by disinformation" are both high-risk, they require different approaches for defending against the threats they are facing. A clear, focused scope will result in a solid cyber defense plan that is context-specific and actionable for these communities.

What cybersecurity harms should CISA try to address and in what order of priority?

Most broadly, the highest priority harms are those which are designed by the adversary to prevent high-risk communities and the organizations supporting them to function effectively and participate in public debates and discussions that are important to those communities. To accomplish these harms, threat actors can use direct attacks to shut down the community's online activities or key voices in the community, as well as indirect threats like information operations to discredit or misrepresent the organization or to conduct surveillance on the community to enable other attacks.

Harms are largely the result of the threat actor's intent. If the goal is to discredit an organization, then compromising and publishing data dumps, planting false evidence, and compromising key figures could be a goal. If the goal is to put the organization out of business, then ransomware and data wiper trojans, targeting of backup infrastructure, account takeover and company impersonation are all strategies. Each of these threat actors may use a variety of attack vectors, including email, call, text message, social media direct message, intelligence gathering for in person attack vectors for those at high-risk.

Focusing on spear phishing, account takeover, and spyware to track people's locations and where they live may be a good place to start to help less resourced individuals and organizations defend themselves from being misrepresented or harmed (e.g., financially, physically, or digitally).

Attacks that might specifically target individuals that make up an organization could include, personal device compromise, dumping of emails, discovering human sources, and information operations to discredit. Each attack vector has different counters, either specific technical steps that could be taken to mitigate a harm, or awareness training or changes in behavior that lowers the risk—such as encrypting a high-risk community member's laptop should it be stolen.

In determining what priority to assign to the different possible harms, the overriding priority should be the protection of life and the minimization of physical harm. To best mitigate against this threat through technical cybersecurity measures, the focus should be protecting against cyberattacks designed to gather information necessary for such in-person threats. For example, cyberattacks designed to infiltrate community members' devices and identify their contacts for later in-person attacks.

As discussed above, another important priority is preventing or mitigating attacks that are designed to undermine the effectiveness of HRC organizations or the high-risk communities themselves. The goal of attacks on civil society is often to discourage or silence opponents and critics, and remove those voices from the public discourse, making this protection a key priority for the HRC.

Secondary priorities should be on those solutions that can scale, such as tools that can be used widely, training that then can be re-taught, reports and information sharing that can be amplified by other organizations. One-off solutions or highly complex solutions, while valuable, should not be the focus at this time.

What cybersecurity offerings should CISA provide and in what order of priority?

It is difficult for HRC to assess risk and understand all of the options available to better protect themselves. Most existing resources on cybersecurity prevention and detection are focused on the broad median risk organizations who are less likely to be targeted by advanced adversaries. The tactics, tools, and procedures attackers apply to high-risk victims are commonly more specialized with an emphasis on bypassing common defenses. There is a need from the high-risk community for better guidance and tools for defending against more advanced attacks. There is no "on-ramp" from the USG for communities looking for help.

The HRC need these on-ramps to find the tutorials, tools, online training, conferences and free services offered by large cloud providers and smaller privacy focused platforms. Moreover, this on-ramp needs to be constantly updated because the threats and some of the associated security advice can change rapidly.

Existing work falls into two broad categories: advisory guidance that details general steps that organizations should take to reduce susceptibility to cyberattacks, and technical measures to resist active compromise.

Among the advisory guidance programs, one of the most well-known is *Shields Up*, which outlines principles for protecting general organizations. Other resources are listed in Appendix C.

Shields Up can be the basis for an expanded offering, making CISA an on-ramp to security measures. CISA could build on the success and visibility of the *Shields Up* guidance and expand it into a "Wizard-like"-resource that will forward organizations of sufficient risk level to further technical security recommendations.

In addition, CISA can identify gaps in mitigations and advocate for the creation of protections. One approach could be to create a "Most Wanted Mitigations" top 10 list based on real world experience of what would better protect high-risk communities, even for more specific cases such as journalism or healthcare organizations that may have specific needs and risk factors.

A *Shields Up* companion resource could be developed for post-compromise recovery (maybe "Shield Repair") that would be extremely useful. CISA could create a series of best practices and resources that civil society can use when the preventive side of this has failed, or when the civil society organization got engaged post-compromise.

These measures would be most effective if CISA ensures that the initiative has resources, staffing, and budget for the long term. For the informational materials, CISA must not just put up a website, but also have the staff and funding necessary to keep it up to date and expand as needed while working with other government and industry partners. This will give confidence to HRC and organizations in general that CISA and the USG has an enduring commitment.

Identifying simple to understand and deploy "lock down" solutions can help the largest number of people. For example, iCloud Advanced Data Protection is a security feature from Apple that disables use of iCloud from the web, a popular vector for attackers, and would help provide protection in the real-world examples of attacks in Appendix A. Among the technical measures, examples include Apple's Lockdown Mode and similar techniques for other operating systems, listed in Appendix D.

One-click lockdown tools have the added benefit of being simple to deploy and use by non-expert users, but there is no accessible list of maintained offerings and the benefits of using them. An example list of such tools is listed in the appendix to this report.

Existing efforts provide a building block for high-risk organizations to increase their security posture, but there are two limiting factors that reduce the effectiveness of these efforts. First, there is a lack of guidance regarding when an organization should deploy these measures. Second, there is no central clearing house that comprehensively surveys available resources. These factors lead not only to uncertainty (especially for low-resourced organizations without dedicated cybersecurity staff) about which security measures to undertake, which hampers the security of these individual organizations, but also to a systemic uncertainty of what mitigation gaps exist in the ecosystem, which hampers the development of mitigations to fill these gaps.

The determination of recommended mitigations can be informed by a self-reported general survey of societal/political (e.g., "Does your organization interface with oppositional media organizations abroad?") and technical (e.g., "Do individuals in your organization use their own mobile devices for organization business?") risk factors.

CISA's recommendations would draw from a CISA-maintained list of technical mitigations, such as those in Appendix C and D, and would ideally include guidance on technical mitigations directly from companies like Apple, Google, Microsoft, Meta, and other platforms/service providers. Ideally, this would mean getting buy-in from tech firms to support and enhance this effort, and CISA is perfectly positioned to be a liaison to these entities.

Offerings generally fall into two categories, the development and sharing of information resources and tools, and the participation with and coordination of other organizations already in the HRCP space.

CISA has an opportunity to become a connector, a clearing house, and a coordinator of other industry and private efforts to protect high-risk communities. By organizing workshops and gathering current best practices, CISA can create guides and online wizards to help people learn of other organizations and training that can help them.

There needs to be guidance to help HRC better understand the tradeoff between keeping all features and protections in a "default" mode for maximum compatibility, and disabling features and deploying lockdown scripts to provide enhanced protection. There are tradeoffs to be made and each HRC will need to determine for themselves what is best. Helping educate them to make an informed decision is critical.

For example, Apple says Lockdown mode is an "optional, extreme protection that's designed for the very few individuals who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats. Most people will never be targeted by attacks of this nature." CISA could provide guidance on how to determine who may need it.

What work already exists in this space and how can CISA be a catalyst for more investment in this work globally?

Because threats to high-risk communities are a critical security challenge, work has already been done in developing mitigations in this space. CISA needs to understand the existing work to help protect high-risk communities, as the most efficient use of CISA's resources would be to act both as a catalyst for expanding and improving the space, support and reinforce existing efforts with an enduring commitment over the long term, and guide HRC to currently available and future mitigations.

The discussions, findings and recommendations above identify both existing projects underway by civil society groups (see Question 2) and within CISA (see Question 4), which can help CISA be a catalyst.

By supporting these existing projects, and extending and expanding existing programs within CISA, CISA will be the most effective in spurring further investment in this space.

In order to make these more effective CISA should work with other internationally focused government agencies (such as the State Department's Internet Freedom program), support domestic NGOs which work with global high-risk communities, and ensure that there are sufficient resources and long-term commitment to its programs. Long term CISA commitment will give the confidence necessary for NGOs and other existing projects to further invest.

What specific actions do you think the USG can take to focus cybersecurity companies and the technology industry broadly on supporting victims?

Technology companies can continue to create features that are easier for less resourced and less technical communities to enable by default. For example, Microsoft offers "S mode", which is designed for security and performance, including exclusively running apps from the Microsoft Store. Google Chromebooks offer a simplified, and safer, experience for using their cloud services.

Targeted communities may be at a disadvantage as they may not understand all the security features of the tools they are using. Attackers have more time and resources to devote to this, with the goal of using those tools to do harm to their targets.

Less technical individuals and low resourced organizations will most likely not have the ability or resources to learn how to properly configure complex feature rich versions of existing technologies (e.g. Microsoft, Google, or Apple). Product vendors offering slimmed down secure-by-default versions of products with specific marketing to consumers and low resourced organizations could help drive those communities to using the modified versions of existing products. Alternatively, vendors could provide guidance tailored to high-risk communities for how to set up and use their platforms in the best way possible.

Recommendations:

- Engage with a diverse set of NGOs that provide support to high-risk civil society organizations. To gain a better understanding of how they support civil society, ask about:
    - What the organization does and how it operates, how it works with civil society organizations, what it offers proactively and why, what it offers reactively, the resources it's able to dedicate to this effort, constraints such as budget, resources, relationships, insight.
    - How CISA and industry partners can help support them by sharing information, connecting organizations for mutual support while promoting their efforts.
- Engage with U.S. nationals who have been targeted by nation-state actors using sophisticated spyware to learn from their experiences.
- Engage with academic researchers that study the security of individuals from high-risk communities to facilitate their interactions with and research on the needs of said high-risk communities.
- Work with the State Department's Internet Freedom program to assist them helping high-risk communities overseas.
- Define the scope of the communities and threats that CISA will focus on initially.
- Initially prioritize entities that can multiply CISA's efforts through "train the trainer" and act as trusted partners and gateways to the smaller entities.
    - Within these entities, focus on those who are serving groups which may be particularly highly targeted by governments and other threat actors.
- Prioritize the protection of life and minimize physical harms.
- Prioritize harms that can stop or undermine the effectiveness of organizations and communities' work in the public sphere.
- Prioritize preventive defense guidance to high-risk communities.
- Push out tools and how-to materials to enable low resourced organizations and individuals to evade spyware used by oppressive governments and violent organizations targeting their demographics.
- Create a high-risk reporting form online that requests certain information and shows people what to watch for and report for assistance in determining if they're being targeted and how aggressive the entity is going about targeting them.
- Identify, promote, and fund tools to help communities and organizations self-assess their cyber maturity and risk levels. For example, look to the Ford Foundation's Cybersecurity Assessment Tool as a starting point.

- Identify, promote, and fund ‘One and Done’ ways to increase protections, such as advanced protection features on phones, with explicit step-by-step instructions.
- CISA should build on the success and visibility of the *Shields Up* guidance and
    - Expand it into a "Wizard-like" resource that will forward organizations of sufficient risk level to further technical security recommendations.
    - Gather information necessary to identify mitigation gaps, and encourage the development of further mitigations.
    - Create a series of best practices and resources that civil society can use when the preventive side of this has failed, or when the civil society organization got engaged post-compromise.
- Field questions from HRC entities as they determine their risk level. CISA would fill a critical lack here, as there is a current significant gap in technical resources for such determination.
- Connect an HRC entity with a list of security vendors, open-source projects, and other resources that may be needed at that entity's risk level. This is a natural effect of CISA's positioning in between these communities.
- Connect government entities with HRC entities for the former to better understand the latter's needs and stature. As a government entity, CISA may carry enough internal weight to effectively support such conversations.
- Connect academics to HRC entities to facilitate academic studies in HRC risk management and defense. CISA's relationship with HRC entities can significantly improve the reach and applicability of academic studies on the topic and augment our understanding of risk among these communities.
- Provide threat modeling information to the HRC community to help them fully understand their threat and what is a worthwhile tradeoff for the loss of functionality for additional tech protections.
- Develop a way to provide information to HRC at an organizational level, as well as high-risk individuals directly.
- Work with partners and industry to alert HRC of detected targeting, such as what Google Gmail does when they detect a foreign adversary attempting to compromise your email account. This alert would warn the end user to move to the next level of protection, provide actionable recommendations for self-help such as revoking other linked device permissions and then signing out and back in to get a new login token.
- Provide a mechanism for people to suggest tools and guidance for CISA to review and include in their recommendations.
- Develop a life cycle to keep in touch with providers and high-risk groups to evolve these recommendations based on real world experiences.
- Continue to enable, require and push for increased security-by-default features turned on for products and devices out of the box especially for end consumers and small or low resourced user base.
- Push product vendors to consider creating slimmed down small org and non-technical user versions of their products and solutions for the end consumer, non-profit and low resourced organizations to move them off of enterprise solutions.
- Create a way to recognize companies which participate in HRC protection programs.
- Promote collaboration amongst these companies to share threat intelligence.

Appendices:

A. In-the-wild Attacks

- Victims of Candiru, Pegasus, Predator: https://github.com/GranittHQ
- FORCEDENTRY NSO Group iMessage Zero-Click Exploit Captured in the Wild - https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
- re:publica 2022: Claudio "Nex" Guarnieri: Pegasus, spyware, and our rights and freedoms - https://www.youtube.com/watch?v=DoueeVHHkOs
- When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users - https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/
- One click attack would be prevented by Lockdown mode, as it disable clicking links in Messages: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
- A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution: https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
- Exploit Archaeology: A forensic history of in-the-wild NSO group exploits: https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Exploit-archaeology-a-forensic-history-of-in-the-wild-NSO-Group-exploits.pdf
- Attacks on Lama Fakih, Roman Gressier, and Artemis Seaford
  https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets
  https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus
  https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html

B. NGOs

- Citizen Lab: https://citizenlab.ca/
- Electronic Frontier Foundation: https://eff.org/
  - (Note: Mr. Kurt Opsahl is a volunteer Special Counsel with EFF)
- Security Education Companion: https://www.securityeducationcompanion.org/
- Internews https://internews.org/areas-of-expertise/global-tech/what-we-do/digital-safety/
- Access Now: https://www.accessnow.org/help/
- Freedom of Press Foundation https://freedom.press/training/
- Committee to Protect Journalists: https://cpj.org/2022/11/digital-safety-using-online-platforms-safely-as-a-journalist/
- Amnesty International: https://www.amnesty.org/
- Superbloom (Simply Secure): https://simplysecure.org/
- Global Forum on Cyber Expertise: https://thegfce.org/
- Level Up: https://level-up.cc
- Library Freedom Institute: https://libraryfreedom.org/lfi/
- Granitt: https://granitt.io/, founded by Ms. Runa Sandvik

C. Risk Management Mitigations

- Ford Foundation's Cybersecurity Assessment Tool (CAT) is designed to measure the maturity, resiliency, and strength of an organization's cybersecurity efforts: https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks/cybersecurity-assessment-tool/
- CISA *Shields Up*: https://www.cisa.gov/shields-up

D. Example Lockdown Tools

- National Checklist Program: https://ncp.nist.gov/repository

- Hardentools simply reduces the attack surface on Microsoft Windows computers by disabling low-hanging fruit risky features: https://github.com/securitywithoutborders/hardentools
- Harden Windows Safely: https://github.com/HotCakeX/Harden-Windows-Security
- Microsoft Security Privileged Access: https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview
- Android Advanced Protection: https://support.google.com/accounts/answer/9764949?hl=en
- GrapheneOS Mobile OS that is Android: https://grapheneos.org/
- Apple Lockdown Mode: https://support.apple.com/en-us/HT212650
- Apple Advanced Data Protection for iCloud: https://support.apple.com/en-us/HT212520
- The MacOS Hardening Project: https://github.com/ataumo/macos_hardening
- Apple configuration profiles: https://it-training.apple.com/tutorials/deployment/dm105

E. Example Posture Management Tools

- Open Cloud Security Posture Management - https://github.com/OpenCSPM/opencspm
- Scout Suite (open source) Multi-Cloud Security Posture Auditing tool https://github.com/nccgroup/ScoutSuite

F. Background Reference Documents

- Secretary Mayorkas Discusses New U.S. Efforts to Counter the Misuse of Technology and the Spread of Digital Authoritarianism at Summit for Democracy, March 30, 2023, https://www.dhs.gov/news/2023/03/30/secretary-mayorkas-discusses-new-us-efforts-counter-spread-digital-authoritarianism
- The Summit for Democracy page, March 30, 2023, https://www.state.gov/summit-for-democracy/
- JCDC Focused on Persistent Collaboration and Staying Ahead of Cyber Risk in 2023, January 26, 2023, https://www.cisa.gov/news-events/news/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023.
- Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression, March 30, 2023, https://www.cisa.gov/news-events/news/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
- CISA's *Shields Up*: Guidance for Organizations page, https://www.cisa.gov/shields-guidance-organizations

Acknowledgements

Technical Advisory Council Subcommittee Members:

Mr. Jeff Moss, Subcommittee Chair, DEF CON Communications
Mr. Dino Dai Zovi, Security Researcher
Mr. Luiz Eduardo, Aruba Threat Labs
Mr. Isiah Jones, Applied Integrated Technologies
Mr. Kurt Opsahl, Electronic Frontier Foundation
Ms. Runa Sandvik, Granitt
Mr. Steve Schmidt, Amazon
Mr. Yan Shoshitaishvili, Arizona State University
Dr. Kate Starbird, University of Washington
Ms. Rachel Tobac, SocialProof Security
Mr. David Weston, Microsoft
Mr. Bill Woodcock, Packet Clearing House
Ms. Yan Zhu, Brave Software

DRAFT REPORT TO THE CISA DIRECTOR

Transforming the Cyber Workforce

September 13, 2023

Introduction:

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Transforming the Cyber Workforce subcommittee to support CISA's efforts to recruit top talent and develop and retain its talented workforce and manage a remote workforce.

Findings:

The outlined recommendations are guided by the six scoping questions provided to the subcommittee by the CISA Director. They are informed by meetings that assessed the current state of CISA's workforce management approach and input from industry leaders and private sector experts on the future of work.

CISA must develop clear benchmarks, metrics, and milestones to track progress, drive traction and measure the long-term cultural changes that will define success in this workstream.

How can CISA measure and improve employee engagement beyond the annual employee engagement survey?
Currently, CISA conducts annual employee engagement surveys through the Office of Personnel Management which we understand standardizes the questions for all federal agencies and maintains sole access to the raw data. As such, CISA is constrained in its ability to measure engagement specific to the CISA workforce or to access the standardized data directly and conduct its analyses. To improve employee engagement in creative, thoughtful ways CISA must collect data that is specific and meaningful for its workforce, with appropriate access to the data and regular, thoughtful analysis of the data.

What programs and initiatives are the private sector using to combat burnout, address unreasonable workload, and support employee wellbeing that CISA could benefit from?
Across the private sector there are several programs and initiatives that are being used to combat burnout, address unreasonable workload, and support employee wellbeing. Addressing these challenges is key to driving employee growth and increasing retention. These are best considered in three buckets: Programmatic Enhancements, Cultural Alignment, and Employee Support.

Which promising practices of a People-First culture to recruit, retain, and continually grow top talent can be applied within a federal government agency?
A People-First culture and the practices it promotes are foundational to the recruitment, retention, and growth of top talent. The Subcommittee is pleased with the progress that CISA has made in this area since delivering its initial set of recommendations and applauds its continued commitment. By aligning to industry-specific standards and frameworks and creating more opportunities for employee feedback, CISA can amplify its culture and better compete for top talent.

What are the best practices for managing and motivating a remote and hybrid workforce, to include ensuring that new employees are effectively integrated into the CISA culture and that all employees embrace the importance of collaboration?
As new employees join an organization, it is critical that they are welcomed and onboarded effectively. This is particularly important for remote and hybrid employees (who comprise a significant portion of CISA's workforce). Through conducting a cultural analysis, giving immediate structure to new joiners, and providing opportunities to engage with senior leaders and teammates, CISA can effectively manage and motivate its workforce.

Which internal mobility programs or career development programs should CISA consider for developing broader competencies and experiences for its cyber workforce?
Career development and mobility are essential in developing broader organizational competencies, growing individual employee skillsets, and increasing retention rates. It is important to provide easy access to a wide variety of enrichment opportunities, develop clear structures and guidance for progression and growth, and establish innovative talent programs in support of these efforts.

How can CISA reskill, upskill, and cross-train its workforce to account for changing needs?
As the cyber threat landscape evolves and new technologies emerge, it is important that CISA has a deliberate approach to reskilling, upskilling, and cross-training its workforce to keep pace. Through the establishment of a senior steering committee and enhancements to the agency's learning and development approach, CISA can ensure that its workforce stays ahead of cybercriminals and emerging threat areas.

Recommendations:

- Work with the Office of Personnel Management to obtain access to relevant and appropriate survey and employee data collected from CISA employees. A short technical sprint, in cooperation with OPM and CISA legal counsel, could provide options for OPM to securely share data with CISA about their employees. CISA must be able to access and analyze survey engagement data from its own employees, for the benefit of its workforce.
- The OPM survey data will be helpful but may not provide everything needed for CISA to strengthen employee engagement. As such, CISA should develop and manage its own approach to developing a full-scope employee engagement survey.
    - It is important that this CISA-driven approach include both a broad annual employee engagement survey and supplementary pulse surveys on a weekly, monthly, or quarterly basis to get a complete picture of employee engagement and sentiment.
        - For these surveys, it would be valuable to use pre-written or provided questions as opposed to creating new questions.
        - These questions can also be used to reinforce CISA's cultural values implicitly through the questions asked.
- Gain access to comparative external employee engagement information for benchmark purposes.
    - The focus of the benchmarking should include: 1) Approaches to measure engagement and 2) Tools used for measurement.
        - Tools used in this space by the private sector include: CultureAmp, 15Five, Lattice, and Betterworks.
- CISA's Chief People Officer and Chief Human Capital Officer should create a working group within the agency, comprised of key leaders and mission support personnel, to continually identify, modify, and validate key metrics CISA uses to measure engagement. Additionally, this group should review and validate the tools used to capture this data.
    - Questions that this group could consider include: 1) What are the metrics used across other government agencies, 2) What are the best practices for engagement used across other government agencies, and 3) What are the limited factors that inhibit engagement and action for CISA employees?
- Drive greater value from CISA's Employee Affinity Groups (EAGs) to support employee wellbeing, build community, and enhance culture.
    - This could look like expanding the number of interest areas or points of connection represented by EAGs or incorporating EAGs into overall personnel development and planning.
- Provide opportunities for employees to start their own EAGs and give them potential access to funding if key membership and activity metrics are achieved.
- Leverage data from programs that provide quantitative detail around current workloads and employee capacity such as Microsoft Viva to gain insight into employee wellbeing and help address unreasonable workloads.

- Implement an employee-driven recognition program that allows employees to recognize each other's exemplary performance, provide a measure of success for achievement, and take an active role in promoting CISA's culture.
- Establish a working group that benchmarks CISA's approach to employee support against the private sector's approach on a regular basis.
    - The working group should be given a mandate to make continual recommendations of best practices and innovative ways to support employee wellbeing.
    - As an initial action, the working group could evaluate and enhance CISA's approach through: 1) Implementing meeting-free days or blocks of time, 2) Reinforcing and re-educating scheduling flexibility approaches that exist within CISA today, and 3) Exploring the potential of incorporating half-day/Summer Fridays as workloads allow.
- Formalize and educate employees on organizational growth paths and career progressions to provide more structure and clarity around development.
- Build a cohort-based continuous learning opportunity to upskill employees in key areas of strategic interest while also driving culture through connection.
    - To strengthen the impact these cohorts have on CISA's culture, cohorts should be cross-functional in make-up.
- Establish internal events (like Capture the Flag competitions) that provide the broader organization with the chance to deepen their cyber skillsets through access to CISA's cyber range or other cyber-specific training tools.
- Create people manager specific training pathways to equip them with the tools needed to support employee wellbeing and reinforce the importance of their role in proactively identifying and addressing employee burnout.
- Leverage the NICE Framework Career Navigation Pathways to align job roles and responsibilities more closely to widely accepted industry framework and make it easier for external talent to join CISA as part of their career progression.
- Create more opportunities for team members to share feedback on their managers to gain insight into leadership effectiveness and empower employees to feel more ownership of CISA's culture.
- Conduct Exit Interviews vs. exit surveys to better understand the motivations of people separating from CISA.
    - The interviews should be designed to gain insight into key questions such as: 1) What has worked in supporting their development and career growth, 2) Where do they see opportunity for improvement, and 3) Would they consider coming back to work at CISA in the future?
- As part of CISA's ongoing efforts to amplify their cultural principles and values, CISA should gather a small working group of key senior stakeholders to identify opportunities for remote and hybrid employees to actively engage with the culture. This will help to drive a sense of cultural ownership and support adoption of the culture.
- Develop a remote/hybrid on-boarding program that provides structure for new employees and a checklist of essential actions, trainings and learning modules that they need to complete.
    - As part of this high-touch onboarding program, each new employee should be given an on-boarding buddy from their team and directed to Employee Affinity Groups.
- Host a weekly welcome meeting for new joiners led by senior leadership to reinforce the cultural messages received during onboarding and make them feel like part of the team.
- Intentionally bring teams together on a regular basis for the kind of collaboration and culture building that is best done in person such as larger meetings, project-specific work and team development days.
- Implement an internal talent marketplace to facilitate internal mobility, help increase transparency and democratize opportunities for career development. A platform like this allows employees to own their own careers while upskilling CISA's workforce.
    - This internal talent marketplace can be used to proactively identify experiences to support the growth path of CISA's top talent by leveraging the gig work mentality that is so prevalent in the tech space.
- Identify career development opportunities that support volunteerism efforts, giving employees the chance to blend their passion and profession while supporting communities that lack the ability or knowledge to effectively secure themselves– including those that are target-rich, cyber-poor such as hospitals, K-12 school districts, or nongovernment organizations (NGOs).

    - As an example, the Cyber Peace Institute has a program called Cyber Peace Builders through which volunteers lend their cyber skillsets to enhance the security of NGOs.
- Develop multi-year strategic development rotations for talent to gain interdisciplinary experience.
    - As part of these strategic development rotations, CISA should provide people managers additional training to help identify suitable candidates for the program.
    - The creation of these strategic rotations should take an incremental approach. To help ensure the quality of these rotations and their sustainable success, the initial focus could first be on a single professional development track aligned to growth paths within the organization, such as Artificial Intelligence. From there, CISA could expand the program to include other areas of strategic interest.
- Support the expansion and usage of a tour-of-duty program that enables talent swapping 1) between CISA and the private sector and 2) within government agencies. As part of this, CISA must gain insight into current program usage, areas of opportunity for improvement, and barriers to usage.
    - Expanded talent swap programs and secondments with high usage rates could serve as a competitive differentiator for CISA and provide a unique offering to help attract top talent.
- Establish a working group of senior CISA leaders to evaluate emerging technologies and incorporate it into their plans to reskill, upskill, and cross-skill the CISA workforce.
    - As part of these efforts, the working group should map these emerging technologies to CISA's strategic priorities and goals and explore the creation of an academy-based learning model.
- Review the current approach to employee development to ensure that employees have access to a variety of relevant and effective trainings that are both experiential, hands-on training and more traditional academic training.

Appendix: List of Contributors to this Report

The following TCW subcommittee members participated in the study and recommendations documented in this report.

Ron Green, Subcommittee Chair, Mastercard
Steve Adler, Former Mayor of Austin, TX
Nicole Perlroth, Cybersecurity Journalist
Nicole Wong, NWong Strategies