DRAFT REPORT TO THE CISA DIRECTOR

Transforming the Cyber Workforce

June 22, 2022

Introduction:

The Transforming the Cyber Workforce Subcommittee has been asked to develop strategic recommendations to identify and cultivate the best pipelines for talent, expand all forms of diversity, and develop retention efforts to keep CISA's best people. Additionally, the subcommittee has been tasked with identifying creative ways to develop a better-informed digital workforce and inspire the next generation of cyber talent through education of "K through Gray" communities.

The recommendations outlined below focus on (1) Addressing CISA's Workforce Challenges and (2) Building the National Cyber Workforce.

Findings:

The outlined recommendations are informed by meetings which assessed the current state of hiring and onboarding within the agency and the Federal Government to close talent gaps across leadership and rank-and-file employees. The recommendations are also informed by input from industry leaders on innovative approaches to enhance the cyber talent pipeline and mobilize tech talent for the public sector.

Many public and private entities have provided recommendations to address our nation's cybersecurity challenges, but only modest action has been taken. As such, CISA must develop clear benchmarks, metrics, and milestones to track progress and drive traction. Following this initial tranche of recommendations, CISA must develop clear internal Key Performance Indicators (KPIs) to demonstrate progress on the recommended actions over the next 6-18 months. CSAC will also develop KPIs to hold CISA accountable over the same period.

The Office of the National Cyber Director is developing a broader, interagency national cyber workforce strategy that will include CISA. The outlined recommendations align with their initial thinking. The recommendations work to address the identified urgent gaps in CISA's and the nation's mission-critical cybersecurity workforce and promote opportunities for intervention and improvement.

Given CISA's statutory authorities, CSAC would like CISA to identify the recommendation on which they are able to act, and the recommendations that require additional legislation by Congress.

Recommendations:

- Addressing CISA's Workforce Challenges: The ability to recruit and retain professionals with mission-critical cybersecurity skills will be CISA's ongoing challenge and greatest asset. The federal cyber workforce crisis has been repeatedly addressed in previous reports (e.g., the 2012 Department of Homeland Security CyberSkills Task Force report), yet hundreds of federal cybersecurity positions remain unfilled and nearly 600,000 remain unfilled in the United States alone[i]. Addressing the workforce crisis has become a critical national security threat that will require urgent and effective streamlining of current recruiting and retention processes and a radical expansion of the cybersecurity talent pipeline through innovative partnerships with universities, community colleges, private training organizations, industry, and other federal agencies. As CISA builds its infrastructure and workforce, CISA must (1) prioritize strategic workforce development; (2) dramatically improve its talent acquisition process to be more

competitive with the private sector; (3) radically expand recruitment efforts to identify candidates across their professional lifecycle; and (4) leverage talent identification and hiring success through interagency collaboration.

- Prioritize Strategic Workforce Development**:** CISA requires a comprehensive review of its current workforce and talent needs to ensure that it is properly aligned with the agency's strategic goals and future growth. The review should include assessment of CISA's policies and processes to support hiring for those needs while better competing with the private sector. The CSAC recommends that CISA:
  - Move urgently to hire a Chief People Officer responsible for working with the Director and senior leadership to advance a unified approach to talent acquisition, establish workforce development priorities, and ensure alignment with professional career paths. The CSAC strongly supports CISA's current plans to do this.
  - Ensure that agency managers have the necessary training, dedicated time, and support to focus on strategic needs and gaps in the hiring process, including recruiting to maintain alignment and drive progress against talent goals across the agency.
  - Identify and certify recruiters, with demonstrated expertise in strategic focus areas, to support the agency's broader recruiting efforts for specialized hiring needs.
- Dramatically Improve Hiring Goals and Process**:** While CISA has made some progress toward improving its talent acquisition process, including the launch of the Cyber Talent Management System, CISA must move with far greater speed and urgency to meet the nation's cybersecurity crisis. The process is lengthy and difficult to navigate both internally and externally, and therefore places CISA at a tremendous disadvantage relative to private sector employers for this critical and highly sought-after talent pool. The CSAC recommends that CISA:
  - Set a goal of 90 days from offer to onboarding for cybersecurity candidates. Currently, this process takes an average of 198 days within the agency[ii].
  - Develop a systemic approach to collecting and analyzing data on candidate pools and hiring processes to benchmark, monitor and improve hiring cycles, using an organizational chart to monitor time to fill, time to hire, source of hire, recruitment funnel effectiveness and diversity of candidate slate metrics.
  - Review hiring goals on a regular basis with senior agency leadership, under the guidance of the Chief People Officer and Chief Human Capital Officer, to ensure they remain aligned with the agency's strategy and needs and are properly directed and budgeted to be competitive with private sector employers.
  - Move away from a rigid, inflexible job classification system to a flexible, adaptable, pool-based talent management approach better aligned with organizational needs and career paths for experienced professionals.
- Radically Expand Recruitment Efforts to Identify Candidates Across Their Professional Lifecycle**:** In order to close CISA's talent gap, the agency's recruitment efforts must reach a broader array of people across the full spectrum of experience. Current recruitment efforts reach only a small portion of the eligible candidates in the nation, limiting the agency's talent acquisition potential. The CSAC recommends that CISA:
  - Expand the recruiting pool by increasing awareness of open roles for internal CISA candidates to other government employees, industry, academia, and cybersecurity training organizations.
  - Establish a standing working group comprised of leaders in the public and private sectors tasked with highlighting leadership opportunities at CISA, advising on cybersecurity recruiting challenges, and ensuring accountability.
  - Partner with universities, community colleges, industry, relevant non-profits, the hacker community, and CISA's network of partners to establish an expanded internship program. These partnerships will identify professionals with mission-critical skills that enables CISA to hire full-time employees from a larger pool of candidates.

        - Conduct a thorough review of the interagency security clearing process to identify paths to streamline and speed up this critical path for CISA candidates. The subcommittee heard consistently that the current, unpredictable suitability process is unnecessarily cumbersome and time-consuming, which is a significant obstacle to hiring.
        - Develop a senior leadership specific hiring strategy that uses all resources at CISA's disposal such as Intergovernmental Personnel Act appointments.
    - Leverage Talent Identification and Hiring Success Through Interagency Collaboration**:** There are currently a number of efforts underway to drive interagency collaboration. By using the information and best practices already uncovered by this work, the agency will be better informed to shape its own talent acquisition process. The CSAC recommends that CISA:
        - Bolster and amplify these ongoing efforts to identify, share, and employ best practices for hiring in cybersecurity.
        - Support the creation of an interagency authority similar to a detailee program to allow CISA to source cybersecurity talent from other agencies and vice versa.
        - Create an internal recruiting tool (e.g., a "LinkedIn for Cyber Talent") that allows CISA and other agencies to tap cyber-skilled Federal personnel and track retention and attrition across agencies.
        - Empower teams leading ongoing interagency collaboration efforts to act with the support of CISA to simplify the sharing and implementation of best hiring and retention practices.

- Building the National Cyber Workforce**:** In addition to building its own direct workforce, CISA must play a key role in building out the broader national cybersecurity workforce. The agency's future depends on it. There is a significant gap in availability of skilled cybersecurity professionals compared to the rapidly growing need. This challenge is not new, but it is worsening. In May 2021, there were approximately 465,000 open cyber roles in the United States[iii]. In the last year, this number has grown by 29%, leaving us with just under 600,000 currently open roles[iv]. Additional bodies of work have examined similar recommendations, so the CSAC suggest that CISA amplify select recommendations. The recommendations regarding Building the National Cyber Workforce are built on two pillars: Education and Service.
    - Education: It is still difficult for many people to access the educational resources they need to pursue a career in cybersecurity. There is a need for creative new upskilling, reskilling and pipeline development programs designed to lower the barrier to entry to a career in cybersecurity. The CSAC recommends that CISA:
        - Support the establishment of a virtual National Cyber Academy (e.g., a "West Point for Cyber") with a CISA Cadet track leading to a traditional degree and multi-year commitment to CISA.
        - Partner with universities, community colleges and industry-supported cyber education providers to develop a "CISA-approved degree" that enables CISA to quickly tap from a qualified pool of students and professionals and allows recipients to demonstrate their cyber aptitude.
        - Partner with the private sector in working with academia to develop clear, foundational security training credentials to be required by academic institutions.
        - Unify the many existing youth-oriented cyber programs under a single Junior Cyber Corp umbrella to reach younger cohorts (e.g., K-12) with quality learning opportunities to train the next generation of the cybersecurity workforce and deepen our talent pipeline. Bringing these programs together will simplify the educational experience and help ensure a consistent knowledge baseline for students.
        - Develop cyber competitions using the President's Cup as a model to reach universities, community colleges, and key industry events such as Black Hat.
    - Service: Today, there are a limited number of broadly available pathways directly into cybersecurity, and even fewer that serve the public interest and evoke a sense of civic responsibility. The development of opportunities that meet these needs will deepen our national cyber talent pipeline, provide critical resources

to those without the expertise or funding to bring these to life on their own, as well as increase public understanding that cybersecurity is a shared responsibility. Additionally, The CSAC recommends that CISA:

- Establish government-sponsored programs that blend public service and cybersecurity education and support the development of similar programs from non-government, private and non-profit organizations.
- Partner with members of the Joint Cyber Defense Collaborative (JCDC) Alliance to create a tour-of-duty "Cyber Force" pilot program to bridge urgent CISA talent gaps, upskill CISA's workforce and support the agency's strategic priority of public-private collaboration[v]. JCDC members should loan out top security practitioners/volunteers for a one-to-two-year tour of duty before returning to the private sector as designated CISA Liaisons to facilitate ongoing public-private collaboration such as threat sharing, especially during "Shields Up" initiatives and cybersecurity crises. To further incentivize broad participation in this program, the CSAC recommends that CISA support legislation to offer tax credits and other similar benefits to participating organizations.
- Build a Peace Corps-like cyber program for college graduates and beyond that incorporates education and service to provide domestic cyber development assistance. This would be a broad-based opportunity for early in career professionals to serve their nation while becoming the foundation for the next generation of the Cybersecurity workforce through the development of skills and experiences in cyber.
- Track the movement of CyberCorps Scholarship for Service recipients through government agencies and set a CISA-specific goal of capturing 50% of scholarship recipients by 2025.
- Partner with Teach for America to create a cybersecurity program built on their existing platform to increase access to cyber content in communities across the United States.

---

[i] *Cybersecurity supply and demand heat map*. Cybersecurity Supply and Demand Heat Map. Retrieved May 18, 2022, from https://www.cyberseek.org/heatmap.html

[ii] Cybersecurity and Infrastructure Security Agency, Aggregated Time to Hire Report. https://www.cisa.gov/hiring-process-faqs.

[iii] Morgan, S. (2021, November 11). *Cybersecurity Jobs Report: 3.5 million openings in 2025*. Cybercrime Magazine. Retrieved May 18, 2022, from https://cybersecurityventures.com/jobs/

[iv] *Cybersecurity supply and demand heat map*. Cybersecurity Supply and Demand Heat Map. Retrieved May 18, 2022, from https://www.cyberseek.org/heatmap.html

[v] Using volunteers to fill the cyber workforce gap is not a new concept. The Homeland Security Act of 2002 authorized DHS Secretary to establish a national technology guard, various states have designated Civilian Cyber Corps, and a similar exchange program was a key Cyberspace Solarium Commission recommendation.

DRAFT REPORT TO THE CISA DIRECTOR

Turning the Corner on Cyber Hygiene

June 22, 2022

Introduction:

The Turning the Corner on Cyber Hygiene (CH) Subcommittee was established to examine how the federal government and industry can collaborate to identify appropriate goals and ensure strong cyber hygiene is easy to execute. This document outlines three recommendations offered by the CSAC and provides background and context on how the subcommittee derived the recommendations.

Findings:

By the end of 2021, the public sector saw an increase of 600% in cybercrime since the beginning of the pandemic.[i] Security incidents in 2021 were often related to supply chain and infrastructure breaches. Incidents have led to the public exposure and stealing of intellectual property and other confidential data. Attackers leveraged vulnerabilities to spread ransomware. Protecting the corporate and private data of Americans, their networks, and businesses is not limited to hardening our individual systems and executing incident response. Protection also requires elevating security across diverse ecosystems and clarifying the multitude of regulatory requirements to which American businesses need to adhere.

Security Requirements

Security requirements are nothing new. Federal, local, and private mandates were made to improve the security posture of all American enterprises. Those requirements are numerous, vary widely, often intersect, and can also conflict. The language used can be convoluted, unclear, overly technical, or simply overwhelming to its audience. The lack of clarity, along with the time it takes to parse relevant information, is cause for concern. When individuals assume technical jargon is understood by all, such security requirements often go undefined and are not acted upon. The actions needed for an entity to follow security requirements are subsequently neglected due to the technical misunderstanding.

Even requirements terminology can become misunderstood in technical jargon, such as “after any significant change in the environment take action to remediate identified deficiencies on a timely basis”[ii] and “alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files”.[iii]

Relying solely on compliance and requirements will not increase the nation's security posture.

Focus

To improve security holistically, data, networks, and businesses need to be secured by elevating security hygiene and focusing security responsibility on the right actions to mitigate cyber risk. CISA must focus on the following areas for security efforts:

- Multi-Factor Authentication (MFA)
- Security Awareness Training
- Vulnerability Remediation
- Security Event Logging
- Incident Response Capabilities

• Resiliency & Recovery

Delivery in each of these areas of focus will go a long way to enhance risk mitigation and cyber hygiene across organizations and individuals.

Recommendations:

- CISA must build out its current MFA campaign by identifying additional vehicles for publicizing "More Than A Password".
    - CISA must work to enable MFA everywhere and be inventive in its publicizing. This is a large, multi-dimensional undertaking and can be interpreted differently across various actors. Numerous technical options exist to move users away from a dependency solely on a username and password. Even within the security community, there are conflicting opinions on the correct course of action regarding MFA.
        - The benefits from enabling MFA are widely known. A recent report from Microsoft estimates that 99.9% of account compromise attacks would be prevented if MFA was in place.[iv] The 2021 Verizon Data Breach Investigation Report states that "61% of breaches involved credentials."[v] A recent internal survey of small to medium sized service suppliers asked "Do you feel that using multi-factor authentication (MFA) makes your personal and business data more secure?" 38.5% responded no, with another 25.3% responding "I don't know". This signals that the value added and impact of MFA is not obvious to users.
        - CISA must brand, market, engage, and support a simple, singular message of "More than a Password" that will be memorable.
            - CISA should initiate the campaign to design original creative content for both digital and print media. CISA should create a dedicated "More than a Password" online hub with not only dynamic and creative web content, but also explicit instructions to users on how to achieve the "More than a Password" objective. A new outreach campaign needs to initially leverage social media via DHS and other government high profile figures/accounts. CISA should engage high profile, private sector companies, and celebrities to echo the campaign and have bounce back messaging to the CISA hub. CISA should target large events, such as sporting events (e.g., MLB, NBA, NHL, etc), Fourth of July Parades, back to school / first day of school outings with digital and print marketing. CISA should create network television / cable broadcasts can air media spots; a type of updated "the more you know" public service announcements. CISA should also deploy digital and print signage in state / municipal high traffic areas (e.g., transit hubs, interstate rest stops, airports).
    - CISA must incorporate messaging that goes beyond advocating or educating users about the dangers of single factor authorization. CISA must focus messaging to dispel the myth that enabling and using MFA is difficult, time consuming, and has diminishing returns.
        - Large organizations have begun adopting MFA by default in their engagements with customers. Salesforce announced they mandated a February 1, 2022 deadline for all account users to implement MFA.[vi] In May 2021, Google announced they would enforce and auto-enable Two-Factor Authentication (2FA) for new users. By February 2022, they had more than 150 million 2FA users for Google accounts,[vii] as well as 2 million 2FA users for YouTube creators. GitHub announced in May 2022 that all users who contribute code on its platform will be required to enable 2FA on their accounts by the end of 2023.[viii] Examples of successful implementations and transitions to the usage of multi-factor authentication should be shared as they occur.

- "More Than a Password" is solution agnostic. As such, it's realistic to gather multiple voices to sign on and subscribe to the common objective of eradicating single factor authentication. CISA must collaborate with a multitude of influential companies, spread across a variety of industries and sectors, to come together to amplify the "More Than a Password" message. That unified voice should express a commitment to it being "the path forward" for the betterment of the American public.
- CISA must utilize mechanisms to disseminate "More Than a Password" that illustrate, in great clarity, the consequences and risks associated with not enabling MFA solutions.
    - In the same way that the American public were made aware of the risks of not wearing seatbelts in cars, the public needs to know that choosing to continue to use just a username and password comes at a price.

- CISA must take all available steps to ensure that companies working with the federal government fully adopt MFA by 2025.
    - CISA must work to obtain commitments across sectors and industry to enable MFA solutions and remove the ability for single-factor authentication. This goal will encompass not only technical solutions, but also the processes, training, communication, and socialization of a new way of being secure online.
    - CISA must work to obtain commitments across sectors and industry to enable MFA solutions and remove the ability for single-factor authentication. This goal will encompass not only technical solutions, but also the processes, training, communication, and socialization of a new way of being secure online.
    - CISA must set the deadline of 2025 to ensure the success of this effort. By having a goal date, the "More Than a Password" messaging is better amplified, and expectations are clearly established and communicated for new requirements to partner with both government and industry. The new branding of "MFA by 2025" advances beyond explaining the security expectations, towards declaring that those not using MFA solutions demonstrate negligence in their business practices.
    - To drive to the adoption of MFA solutions by 2025, CISA must establish mechanisms to make this transition a reality. CISA must create and implement the following mechanisms:
        - CISA will garner a commitment from numerous influential high-tech companies to enable MFA by default on their products and services. This coalition can come together and collectively enable this new default functionality at the same time, as an "industry move." CISA will feature these companies as industry partners of government.
        - The CISA coalition will publicly communicate its support of the CISA commitment to "MFA by 2025" initiative.
        - CISA will enlist non-profits, educational institutions, national, state, local and tribal governments, and the extended security community to amplify and publicly support the narrative that single factor authentication is eradicated by 2025.
        - CISA will work closely with small and medium-sized businesses (SMBs) to help them move beyond passwords. An avenue for this can be through additional guidance on CISA's public-facing website.
        - Through CISA, the US Government will lead by example and ensure that government agencies have a path forward to meet the goal of having "MFA by 2025."

- Recommend that CISA launch a "311 National" campaign, to provide an emergency call line and clinics for assistance with cyber incidents for small and medium businesses.

- Across the country, municipalities have leveraged the "311" model as a tool to connect residents, businesses, and visitors to Customer Service Representatives ready to help with general government information and services.
    - CISA must adopt a 311-like experience that acts as a security lifeline. If a small business or member of a local community believes they need support due to a security breach, compromise, or attack, where can they turn? "311 National" envisions locally managed support structures across the nation that are staffed with security response personnel who can assist those in need by providing education, guidance, and real incident response efforts. This will serve as a 311 helpline for information security issues.
    - A combination of local government agencies, higher education institutions, and help from the private sector must come together with security awareness content, incident response playbooks, staffing support, and community outreach / engagement mechanisms. City services, such as 311 lines, government websites, and/or mobile applications that are already in place for citizen engagement would become the proxy for connecting with those in need.
    - CISA should communicate with the city of Austin and the University of Texas who are currently prototyping and testing this idea. In the long-term, once the idea is proven to have impact and value, CISA could reproduce the service in major metropolitan areas across the United States.

Conclusion:

The recommendations outlined above are the initial steps in a long journey toward securing the American public and businesses. CH work is expected to continue for the next six months as CSAC continues to work on recommendations for the remaining scoping questions.

Beyond, CSAC will apply extra efforts towards the remaining recommendations of:

- Security Awareness Training
- Vulnerability Remediation
- Security Event Logging
- Incident Response Capabilities
- Resiliency & Recovery

Appendices:

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

- George Stathakopoulos, Chair
- Alex Stamos
- Nuala O'Connor
- Steve Schmidt
- Bobby Chesney
- Matthew Prince

Member subject matter experts:

- Matt Kehoe
- Jordana Siegel

Other contributors:

- Big Thanks to Mayor Steve Alder and the City of Austin

[i] CompTIA Blog, dated 04/21/2022 - https://connect.comptia.org/blog/cyber-resiliency-begins-with-people-and-process-not-technology
[ii] Unified Compliance, https://www.unifiedcompliance.com/products/search-controls/control/12497/
[iii] Unified compliance, https://www.unifiedcompliance.com/products/search-controls/control/12045/
[iv] Microsoft Blog, dated 08/20/2019 - http://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
[v] Verizon's 2021 Data Breach Investigations Report – https://www.verizon.com/business/resources/dbir/2021/masters-guide/
[vi] https://security.salesforce.com/mfa
[vii] https://blog.google/technology/safety-security/reducing-account-hijacking/
[viii] https://github.blog/2022-05-04-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/

DRAFT REPORT TO THE CISA DIRECTOR

Technical Advisory Council

Vulnerability Discovery and Disclosure Recommendations

June 22, 2022

Introduction:

The Technical Advisory Council Subcommittee was established to leverage the imagination, ingenuity, and talents of technical experts from diverse background and experiences for the good of the nation. The subcommittee was asked to evaluate and make recommendations tactical and strategic in nature. These Cybersecurity Advisory Committee (CSAC) recommendations for the June Quarterly Meeting focus on vulnerability discovery and disclosure.

CSAC conducted interviews with sector-specific agencies such as the Food and Drug Administration (FDA), product vendors, and CISA staff to determine the current state of vulnerability discovery and disclosure practices across government and industry and provide meaningful recommendations.

The act of disclosing a security vulnerability for an impacted system at first seems simple: Contact the maker or party responsible for a hardware or software system and report the problem. Unfortunately, in today's world it is not that simple, with competing equities, jurisdictions, regulations, legalities, and sometimes no clear reporting contact. Some manufacturers are responsive to reports, while others are hostile. What if the manufacturer can't be located or no longer exists?

The reporting party now has an ethical dilemma. They could stay silent while everyone dependent on the vulnerable system continues to use it, oblivious to the risk. They could make a public announcement revealing the vulnerability to put everyone on notice while also putting everyone at risk.

In this environment, CISA, acting as the nation's civilian defense agency, has the opportunity to improve the disclosure process through improved coordination, collaboration, and making the process more attractive to researchers, academics, and hackers wishing to do the right thing by reporting vulnerabilities.

Findings:

CISA is best positioned to support, enable, facilitate, promote, and shepherd collaboration between effected parties including asset owners, sector specific agencies, state, local, tribal, territorial, international government partners, product vendors, and security researchers to reduce the exposure of the nation to emerging cyber security threats. CISA should communicate cross-sector norms and baselines and work with sector-specific agencies to determine impact. CISA should provide existing tools and training that facilitate collaboration and transparent workflows between stakeholders in the vulnerability discovery, resolution, and coordinated disclosure lifecycle.

The challenge for CISA is to determine how to add value by increasing coordination and reducing duplication of effort. Some sector-specific agencies already operate their own incident response centers, including coordinating and sharing information with organizations in the particular sector. The maturity of the sector-specific agencies varies depending on budget, availability of scalable staff, how well they have integrated their workflows with others, etc.

It is not uncommon for researchers reporting vulnerabilities to be individual contributors, and as such have limited time and energy to navigate complex or lengthy vulnerability coordination processes. The more they are tied up with bureaucratic requirements, the less likely they are to want to engage with the disclosure process in the future. Reducing friction for those disclosing is important in creating a healthy ecosystem of researchers. If it is too difficult to report the vulnerability, the risk of researchers publicly disclosing or not reporting at all, increases.

Effective vulnerability programs are engaging, transparent, timely, properly staffed, and have a proactive feedback loop between product teams, security researchers, and sector-specific agencies. Each one of these elements offers an opportunity to improve the overall effectiveness of the program. For example, successful vulnerability disclosure programs rely on a number of incentives to attract researchers to their program. Such incentives include bounty payments, public recognition of their contribution, and professional and peer respect.

Recommendations:

CISA should implement the following actions in the respective timeframes to include:

- Develop incentives and access to information to aid security researchers who will submit vulnerabilities affecting critical systems. Examples include:
    - Grow the pool of potential researchers through work visa sponsorships and streamlined training opportunities.
    - Encourage continued participation by providing rewards such as public recognition and cash awards.
    - Make vulnerability reporting beneficial to researcher careers through internships and career networking opportunities.
    - Work with Congress and the Department of Justice to reduce legal liabilities for those wishing to report vulnerabilities with good faith, such as the DMCA exceptions for security research[i].
    - Standardize the reporting experience to reduce the back and forth necessary to clarify details.
    - Encourage the use of RFC 9116, security.txt which describes how to create a standardized way to inform security researchers on how to report a vulnerability[ii].
        - For the Federal civilian agencies for which CISA has strong authorities, make this a mandatory requirement.

- Encourage an environment that works to enable frustration-free vulnerability research and reporting.
    - Work with Congress and sector-specific regulatory agencies to require that manufacturers supply firmware images of every released version for the industry, which should be ultimately archived for future automated analysis.

- Invest in a central platform to facilitate the intake of suspect vulnerabilities and communication between security researchers, agencies, and vendors:
    - In order to help provide security researchers with a 'one-stop-shop' that will enable better disclosures and help them navigate government bureaucracies.
    - To improve visibility, transparency, communication, and resolution of vulnerabilities that affect multiple critical sectors.
- Simplify the reporting process and provide feedback to those reporting. Streamline the process to triage reported vulnerabilities and streamline the reporting process to reduce later uncertainty.

  - CISA should invest in a centralized role in coordinating with sector-specific agencies, to ensure high quality evaluation and communication of vulnerabilities identified in products in their sector constituents.
  - Ensure security researchers have visibility into the triage status of vulnerabilities they have submitted in the workflow.
  - Enhance information sharing by create interagency workflows with sector-specific agencies, product vendors, asset owners, and trusted security researchers.
  - Mitigate barriers to the technical community working with CISA by promoting, and improving upon, the existing portals such as Vulnerability Information and Coordination Environment (VINCE) to target specific industries.
  - Support and promote key industry-specific international security standards and actively participate in their working groups. For example, part 4-1 of ISA/IEC 62443, which requires product vendors to have Product CERT teams that include support and collaboration for vulnerability disclosure and discovery would enhance industry coordination, and CISA could participate in the 62443 committee working groups.

- Improve the notification processes after a disclosure has been verified and acted on.
  - Standardize the way in which reports are disseminated, in both human and machine-readable formats.
  - If applicable, connect the disclosure to the existing ATT&CK Framework[iii].
  - Ensure the disclosure information is easily searchable and can be sorted by make, model, brand, versions, and impacted sectors. Work with the community to leverage open-source projects (e.g., Industrial Control Systems (ICS) Advisory Project) and past ICS-CERT and US-CERT page approaches.

Conclusion:

The Vulnerability Disclosure lifecycle in complex, depending on human interactions and judgement calls on how critical a disclosure may be. Standardizing as many steps as possible while considering the burden of disclosure can help reduce the friction to researchers. Better coordination between parties, through automation or more actionable notices, will help reduce the gap between when a disclosure is made and when a defensive action can be taken.

CISA, acting as a coordinator and source of trusted expertise, is in a unique position to improve the Vulnerability Disclosure Process not just for Department of Homeland Security or the civilian federal government, but to act as a model for everyone.

The committee will continue to interview necessary stakeholders and provide more research, observations, feedback, and recommendations that will enable CISA to better serve the critical infrastructure community and provide greater incentives and experiences for security researchers to continually improve responsible discovery and disclosure.

Cyber Threat Intelligence Sharing Recommendations

Introduction:

The Technical Advisory Council Subcommittee was established to leverage the imagination, ingenuity, and talents of technical experts from diverse background and experiences for the good of the nation. The subcommittee was asked to evaluate and make recommendations tactical and strategic in nature. These Cybersecurity Advisory Committee (CSAC) recommendations for the June Quarterly Meeting focus on cyber threat intelligence (CTI).

CTI is leveraged by Defenders, Blueteams, Security Operations, and Information Technology staff small and large as a means to narrow the superset of potential threats and adversaries to a smaller, actionable set. In best case scenarios, high-quality threat intelligence shared in a timely and efficient manner will enable defenders to take actions. When positioned within a simple Protect, Detect, and Respond security framework, cyber threat intelligence has the following value proposition:

- Protect:
  CTI can be used to increase the security posture of entities including blocking traffic associated with an inbound threat, hardening specific configurations associated with an attack, patching, and reducing attack surface. CTI can also assist in identifying new patterns of attack which require additional controls.
- Detect:
  CTI, including Indicators of Compromise (IOC), can be used to analyze and hunt for adversary activity in an environment helping to scope the broad set of threats being monitored into a known set of active threats.
- Respond:
  Connected to detection, actionable IOCs can help Data Forensics and Incident Response (DFIR) and adversary eviction by sharing IOCs and general intel on how to remediate an active threat.

Given a general understanding of the value of effective threat intelligence, what role could and should CISA play in helping to distribute and disseminate threat intelligence? CISA is in a unique position of influence and centrality which enables an organization to curate, arbitrate, and disseminate high quality threat intelligence across the government and private sector due to its mandate, authority, and position of trust.

CSAC recommends that CISA continue to invest in this capability as it has a proven value. CISA must make this CTI capability effective for its consumers across government and private sectors.

Findings:

Currently, CISA has multiple programs with the goal to effectively facilitate dissemination of threat intelligence artifacts including:

- Cyber Information Sharing and Collaboration Program
- Automated Indicator Sharing

The CSAC has reviewed the documentation related to both programs and was able to understand its goal and challenges directly from the stakeholders within this program.

Based on this initial information, the CSAC has identified several opportunities for improving the effectiveness of its intel sharing program for private and public sector users. The following areas of improvement include:

- Consumption of CISA cyber threat intelligence is currently a manual process for many organization.
  - Not every organization has the resources, infrastructure, or expertise to consume and apply much needed threat intelligence in defense in an automated and scalable manner. This limits the impact of the programs.

- Threat intelligence is optimized for detection and its current form is less useful for prevention and response which is a missed opportunity for impact.
    - The format and content of CTI deliverables like IOCs require a lot of knowledge and expertise on the part of the user to convert information into a form that can be applied as prevention capabilities. Examples include endpoint device and Operating System policy changes or infrastructure configuration to reduce the attack surface.
    - Similarly, current IOCs are not optimized for DFIR or recovery and lack critical details for response.

- Smaller organizations, like local governments, lack the tools, infrastructure, and expertise to apply threat intelligence for either detection or proactive controls.
    - Inconsistent capabilities across potential end users of threat intelligence limit the ability for it to have consistent application and thus impact. Many state and local governments have a need for defense and an understanding of the applicability but lack resources and expertise for security infrastructure.
    - While free and/or opensource software instances of critical defense software like threat intelligence management, endpoint detection and response, network monitoring, and Security Information and Event Management (SIEM) capabilities exist, many users may not be aware of them or have a simple mechanism to apply and deploy these capabilities.

- Indicators are not consistently enriched.
    - CISA is in a unique position at the nexus of private and public cybersecurity defense networks and communities. This means there is an opportunity to facilitate both technical enrichment (dynamic analysis, automated data intersection) and crowd sourcing of intel (comments, tagging, confidence votes) to improve the scope and impact of CTI indicators and make the Nation as a whole more secure. Today, only the base indicators are shared leaving an opportunity for impact.

These four problem areas are based on an initial assessment of CISA's threat intelligence sharing programs. More research, interviews, and analysis are required to identify more concrete challenges.

Recommendations:

- Invest in a program to make "threat intelligence as a service" available to all qualified users.
    - A portal which provides a fusion of indicators, automated feeds, crowd source comments, tagging, and enrichment with dynamic analysis would be a force multiplier for defenders who lack the resource or skill to create their own infrastructure. An example of a public service that exhibits many of these capabilities is Virustotal. A comparable service run by CISA and optimized for threat intelligence over malware analysis could have considerable impact and address many of the existing gaps.
    - Reducing the barrier to entry for consumption and application of threat intelligence will broaden its reach and impact smaller organizations, in particular.

- Invest in enriching threat intelligence reports to be more applicable across the three key layers of defense.
    - Non-durable IOCs, like Domain Name System or Internet Protocol information, have a limited time-to-live and are easily circumvented by attackers. If CISA was to increase focus on development and distribution of additional artifacts like group policy and configuration management scripts, and automated attack surface tooling given its unique view across industry and government, it would have a larger impact in defense by preventing attacks.

- Develop and distribute a common opensource stack available to all.
    - Providing simple-to-download virtual machines or containers that include preconfigured threat intelligence management, SIEM, network analysis, and Endpoint Detection and Response agents along with training information would allow broader reach and impact of threat intelligence. This would enable smaller organizations to consume from CISA not only the information on threats but the means to apply this information in defense.

- Explore techniques to enable scalable and effective development of expertise in CTI.
    - Related areas of cybersecurity, such as Vulnerability Research and Penetration Testing, have mature and scalable educational resources, frameworks, and platforms that help in developing needed talent. However, analogous resources for CTI seem to be limited and ad hoc. CISA can encourage the development of and improve the visibility of comprehensive training material, aligned with the technical suggestions above, that could be used by smaller organizations to upskill existing talent.

Conclusion:

CISA is in a unique position to help all organizations in the U.S. become more secure by providing a real-time Threat Intelligence platform that not only has actionable IOCs but is also easily integrated with existing technology used by public and private organizations across the board. The CSAC will continue to investigate opportunities for improving CISA threat intelligence capabilities as the CSAC moves from draft to final form.

References:

1) *Vulnerability Information and Coordination Environment*
2) *Adolus: Framework for Analysis and Coordinated Trust*
3) *Finite State*
4) *NetRise Turbine: Next-Generation Firmware & IoT Security Platform*
5) *ICS Vulnerability Advisory Project Portal*
6) *Assessing the Potential Value of Cyber Threat Intelligence Feeds - Watson*
7) *Data-Driven Threat Hunting Using Sysmon - Vasileios Mavroeidis*
8) *MISP - Open Source Threat Intelligence Framework*
9) *Using Open Tools to Convert Threat Intelligence into Practical Defenses: Threat Hunting Summit 2016*

[i] https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act#Anti-circumvention_exemptions
[ii] https://www.rfc-editor.org/rfc/rfc9116
[iii] https://attack.mitre.org/

Appendices (pertains to both Recommendation areas):

Acronyms

ACRONYM	DEFINITION
CERT	Cyber Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
CVD	Coordinated Vulnerability Disclosure
DFIR	Data Forensics and Incident Response
DOE	Department of Energy
FDA	Food and Drug Administration
ICS OT	Industrial Control Systems Operational Technology
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IOC	Indicator of Compromise
ISA/IEC	International Society of Automation / International Electrotechnical Organization
IT	Information Technology
OS	Operating System
SIEM	Security Information and Event Management
TAC	Technical Advisory Council
TI	Threat Intelligence
TSA	Transportation Security Agency
US-CERT	US- Cyber Emergency Response Team
VINCE	Vulnerability Information and Coordination Environment

Acknowledgements:

Technical Advisory Council Members:

Mr. Jeff Moss, Subcommittee Chair, DEF CON Communications

Mr. Dino Dai Zovi, Cash App

Mr. Luiz Eduardo, Aruba Threat Labs

Mr. Isiah Jones, National Resilience Inc.

Mr. Kurt Opsahl, Electronic Frontier Foundation

Ms. Runa Sandvik, Security Researcher

Mr. Yan Shoshitaishvili, Arizona State University

Ms. Rachel Tobac, SocialProof Security

Mr. David Weston, Microsoft

Mr. Bill Woodcock, Packet Clearing House

Ms. Yan Zhu, Brave Software

Briefers and Other Subject Matter Experts:

Ms. Lindsey Cerkovnik, CISA Cybersecurity Division Vulnerability Disclosure

Mr. Jay Gazlay, CISA Cybersecurity Division Vulnerability Disclosure

Mr. Jeremiah Glenn, CISA Cybersecurity Division

Mr. Eric Goldstein, CISA

Ms. Aftin Ross, U.S. Food and Drug Administration

Mr. Rob Suarez, Becton, Dickinson, and Company

Ms. Nastassia Tamari, Becton, Dickinson, and Company

Ms. Jessica Wilkerson, U.S. Food and Drug Administration

Mr. Beau Woods, CISA

DRAFT REPORT TO THE CISA DIRECTOR

Protecting Critical Infrastructure from Misinformation and Disinformation

June 22, 2022

Introduction:

CISA's mission is to strengthen the security and resilience of the nation's critical functions. The spread of false and misleading information can have a significant impact on CISA's ability to perform that mission. CISA should take a similar risk management approach to these risks that it takes to cybersecurity risks.

Borrowing from a growing body of research[i], we define misinformation as information that is false, but not necessarily intentionally so; disinformation as false or misleading information that is purposefully seeded and/or spread for a strategic objective; and malinformation as information that may be based on fact, but used out of context to mislead, harm, or manipulate. The spread of false and misleading information poses a significant risk to critical functions like elections, public health, financial services, and emergency response. Foreign adversaries intentionally exploit information in these domains (e.g., through the production and spread of dis- and malinformation) for both short-term and long-term geopolitical objectives[ii]. Pervasive MDM diminishes trust in information, in government, and in the democratic process more generally.

The initial recommendations outlined below focus primarily on mis- and disinformation (MD) about election procedures and election results. Future recommendations may seek to address the potential impacts on other critical functions and some of the unique challenges in identifying and countering malinformation.

The First Amendment of the Constitution limits the government's ability to abridge or interfere with the free speech rights of American citizens. The First Amendment and freedom of speech are critical underpinnings to our society and democracy. These recommendations are specifically designed to protect critical functions from the risks of MD, while being sensitive to and appreciating the government's limited role with respect to the regulation or restriction of speech.

CISA is uniquely situated to help build awareness of MDM risks and provide a robust set of best practices related to transparency and communication when addressing mis- and disinformation, specifically in the election context.

Findings:

In addition to researching the issue of MDM more broadly, our committee gathered input from election officials, many of whom are acutely struggling to address mis- and disinformation. Election officials, especially those in small jurisdictions, often lack the training and resources to identify and address the spread of false claims, which is becoming an increasingly demanding aspect of their jobs. Meanwhile, mis- and disinformation are undermining trust in their work and leading to personal harassment and even physical threats.

> **"Responding to misinformation is my day job. My night job is running elections."**
>
> **— Stephen Richer (Recorder, Maricopa County AZ)**

Recommendations:

CISA is positioned to play a unique and productive role in helping address the challenges of MD, especially regarding its mission of protecting election-related critical infrastructure.

- CISA should focus on MD that risks undermining critical functions of American society including:
  - MD that suppresses election participation or falsely undermines confidence in election procedures and outcomes.
  - MD that undermines critical functions carried out by other key democratic institutions, such as the courts, or by other sectors such as the financial system, or public health measures.
  - MD that promotes or provokes violence against key infrastructure or the public.
  - MD that undermines effective responses to mass emergencies or disaster events.

- In this work, CISA's activities should be similar to the Agency's actions to detect, warn about, and mitigate other threats to critical functions (e.g., cybersecurity threats).
  - The initial recommendations focus primarily on MD about election procedures and election results. In the elections context, false information about when, where, and how to vote can disenfranchise voters and the proliferation of false and misleading claims about election processes can reduce confidence in results. More problematically, the proliferation of false and misleading claims about elections can make it difficult to identify and counter any real threats to election integrity, such as from foreign adversaries that leverage disinformation as part of a multi-dimensional attack on election infrastructure.
  - Currently, many election officials across the country are struggling to conduct their critical work of administering our elections while responding to an overwhelming amount of inquiries, including false and misleading allegations. Some elections officials are even experiencing physical threats. Based on briefings to this subcommittee by an election official, CISA should be providing support — through education, collaboration, and funding — for election officials to pre-empt and respond to MD. The specific recommendations below detail how CISA can do this.

- CISA should consider MD across the information ecosystem.
  - In the last decade, the challenge of MD and its threat to democratic societies has become increasingly salient around the globe, including here in the United States.[iii] The Internet, and in particular social media platforms, have played a complex role in this rise — from disrupting the role of traditional "gatekeepers" in the dissemination of information; to vastly accelerating the speed and scale at which information travels; to providing new vectors for manipulation and access for "bad actors" to vast audiences. Researchers are still working to understand the contours of the relationship between social media and MD, even as the platforms themselves — and the norms that guide use on them — are ever-changing. And it is important to note that the outsized attention paid to social media regarding these issues may not accurately represent the proportionality of their role. These sites are part of a broader ecosystem that includes other online websites (e.g., state-run media like Russia Today (RT) – an American branch of Russian state-funded media network) and gray propaganda networks associated with Russia, China, and Iran) and more traditional media (e.g., AM radio and cable news). The problem of MD manifests as information activity across many different parts of this ecosystem.
  - CISA should approach the MD problem with the entire information ecosystem in view. This includes social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio, and other online resources.

- CISA should work across four specific dimensions of MD to include:

- Building Society Resilience to MD. CISA should continue serving a mission of building resilience through broad public awareness campaigns about the challenges of mis- and disinformation and strategies for the public and other specific audiences (e.g., election officials, journalists, etc.) to use to build individual and collective resilience. Here, the focus should be both on enhancing information literacy for the modern information environment and on supporting and integrating civics education into those efforts. Information literacy should include understanding the dynamics of the modern information space (social networks, influencers, and algorithms), understanding and identifying tactics of manipulation, and generally becoming savvier participants in interactive information spaces. The goal should be to both teach people the skills (*how* to identify mis- and disinformation) and provide motivation for using those skills (*why* they don't want to engage with and/or spread mis- and disinformation). This dimension aligns with the CISA's "Cyber Hygiene" mission.

- Proactively Addressing Anticipated MD Threats. CISA should also look at ways to anticipate and mitigate the impact of specific content and narratives impacting its mission of protecting critical functions. These efforts include proactively addressing anticipated threats through education and communication. They require applying knowledge learned from responding to past mis- and disinformation to anticipated, future events. Where possible, CISA should proactively provide informational resources — and assist partners in providing informational resources — to address anticipated threats. In cases where specific narratives are anticipated, CISA should help to educate the public about those narratives, following the best practices suggested by the most recent research. (The research on "debunking vs. prebunking" is ongoing, so CISA must stay up to date on the current recommendations.) Proactive work should also include identifying and supporting trusted, authoritative sources in specific communities (e.g., in the elections context, local media and election officials). These efforts should also include building knowledge and experience that can empower individuals to be more resilient against divisive and despair-inducing disinformation. CISA should support these efforts by creating and sharing materials; by providing education and frameworks for others to produce their own materials; and through funding to local election officials and external organizations to assist in this work.

- Rapidly Responding to Emergent and/or Persistent Informational Threats: CISA should also work to rapidly respond — through transparency and communication — to emergent informational threats to critical infrastructure. This will require a system of rapid identification, analysis, and applying best practices to develop and disseminate communicative products. CISA should work with and provide financial support to external partners who identify emergent informational threats and utilize its strengths in developing and disseminating communicative products to address false and misleading narratives. CISA should also prioritize, where possible, boosting first-hand, trustworthy, and authoritative sources (e.g., election officials) in their efforts to rapidly respond to informational threats. CISA should also be a place where people can find out how to tap into credible sources, governmental and non-governmental. These response efforts can be actor-agnostic, but special attention should be paid to countering Rapidly Responding to Emergent and/or Persistent Informational Threats: CISA should also work to rapidly respond — through transparency and communication — to emergent informational threats to critical infrastructure. This will require a system of rapid identification, analysis, and applying best practices to develop and disseminate communicative products. CISA should work with and provide financial support to external partners who identify emergent informational threats and utilize its strengths in developing and disseminating communicative products to address false and misleading narratives. CISA should also prioritize, where possible, boosting first-hand, trustworthy, and authoritative sources (e.g., election officials) in their efforts to rapidly respond to informational threats. CISA should also be a place where people can find out how to tap into credible sources, governmental and non-governmental. These response efforts can be actor-agnostic, but special attention should be paid to countering foreign threats.

  - Countering Actor-Based Threats**:** CISA should work collaboratively to identify, communicate, and address actor-based MD threats (e.g., foreign and/or criminal MD campaigns that target critical infrastructure).
  - The prioritization of these different aspects of the mission will necessarily be dynamic. During non-election periods and absent other pressing concerns or crises, the primary focus should be on resilience and proactively addressing anticipated threats. During the election period and other active events, the focus shifts to addressing specific and sometimes emergent informational threats through rapid communication.

- On the proactive dimension, CSAC recommends two time-sensitive items related to the 2022 election to include:
  - CISA should support local election officials in producing a "What to Expect on Election Day" plan to proactively address misleading narratives that may arise due to the specific contours of their election materials and procedures, such as through education and communication. This work could include direct collaboration or building educational materials and templates that election officials can use to generate their own plans and resources.
  - CISA should convene a 2022 "What to Expect on Election Day" workshop, to bring together representatives from government agencies and social media platforms, legacy media including local journalists, researchers, and election officials to map out, plan for, and stage resources to address informational threats to the 2022 election (in August 2022) and the 2024 election (convene by April 2024).
  - On the response dimension, during the 2022 election, CISA should continue to proactively participate— in collaboration with outside researchers and those with first-hand authoritative information—in correcting MD that poses a significant threat to critical functions. If possible, CISA should also support external organizations doing MD response work in their own communities — especially organizations in specifically targeted communities, including veterans, faith communities, the Black and Latino communities, immigrant communities, etc. — with grant funding.
  - In doing this work, CISA should operate with the following principles to help build trust in the work and its role:
    - Transparency: Processes, participants and sources of information should be transparent.
    - Collaboration: CISA should prioritize collaboration, not only amongst the different government agencies supporting this work, but also by bringing in civil society, academia, and industry.
    - Speed/Accuracy: Time is of the essence in this work and CISA should act with speed, while being deliberate, accurate and thoughtful.

- CISA should work internally and with collaborators to develop metrics for measuring the impacts of its efforts.
  - To understand the impacts of MD and the efficacy of counter-MD efforts, society needs to develop new metrics, new methods of analysis, and new infrastructure to measure the often diffuse effects of manipulation in a complex sociotechnical system. Though a particular case of MD can have acute impact, some of the more pervasive effects can manifest over long time periods and with both direct and indirect dimensions. This presents a challenge for measuring both impact and mitigation efforts[iv].
  - More research should be done to identify measurable indicators of impact, but initial metrics may include:
    - For general resilience work and proactive messaging: Measuring the spread and engagement of specific CISA campaigns and/or messages. Measuring the efficacy of certain messages (in reducing engagement by participants in MD content).
    - For proactive work: Measuring the size and strength of the networks built (of key stakeholders, trusted sources, and voices, etc.).
    - For rapid response: Measuring how long it takes to respond, the reach of the response, and the number of threats addressed.

    - For actor-based threats: Measuring the number of threats identified and/or addressed, the time to respond, and the impact of the response (e.g., on the activities of the identified actors).

- CISA should invest in external research to assess the impact of MD threats and the efficacy of interventions.
    - More research is needed to develop models and methods for assessing the direct and indirect effects of MD on society. CISA should support this research, through funding and, where appropriate, collaboration. For example, CISA should consider funding third-party research to measure the reach and efficacy of their counter-MD activities. CISA should also support efforts to increase the transparency of social media platforms to enable more research into impacts and interventions online.

---

[i] Jack, Caroline. "Lexicon of lies: Terms for problematic information." Data & Society 3, no. 22 (2017): 1094-1096. ; Wardle, Claire, and Hossein Derakhshan. "Information disorder: Toward an interdisciplinary framework for research and policymaking." (2017). ; Starbird, Kate, Ahmer Arif, and Tom Wilson. "Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations." Proceedings of the ACM on Human-Computer Interaction 3, no. CSCW (2019): 1-26.
[ii] Rid, Thomas. Active Measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux, 2020.
[iii] Spaulding, Suzanne E., Eric Goldstein, and John J. Hamre. Countering Adversary Threats to Democratic Institutions: An Expert Report. Center for Strategic & International Studies, 2018.
[iv] Rid.

DRAFT REPORT TO THE CISA DIRECTOR

Strategic Communications

June 22, 2022

Introduction:

The CSAC Strategic Communications (SC) Subcommittee was tasked to evaluate and make recommendations on expanding CISA's reach with critical partners to help build a national culture of cyber resilience. The recommendations below aim to help promote CISA as a willing and collaborative partner, working arm-in-arm with partners to understand, manage, and reduce risk to cyber and physical infrastructure.

Findings:

CISOs, CIOs, and media representatives have informed the outlined recommendations to better understand the perception of CISA, explore opportunities to improve cyber resilience for the U.S. public, and gauge willingness to participate in campaigns. Based on this work, CISA should implement the following recommendations: (1) "More than a Password" Partnership Program; (2) 311 call line; and (3) building a broader base of support.

Recommendations:

- CSAC recommends that CISA create a **"More than a Password" Partnership program** with Fortune 500 companies. The following steps to roll-out the plan should be considered:
  - CISA should assign a program manager to create the partnership program and work with companies on the best way to amplify the campaign message.
  - CISA should devote resources to creating a "More than a Password" partner portal, marketing materials, including a website and collateral materials.
  - CISA should establish success metrics (e.g., number of companies enrolled in partnership program, etc.).
  - CISA should develop a campaign for "More than a Password" with identified target audiences including:
    - Kids Cyber Education campaign,
    - Senior Cyber hygiene campaign,
    - Celebrity endorsements for campaign, and
    - Faith-based organizations campaign.
  - Once the partnership program is established and meets the outlined metrics, CISA should consider targeting other affinity groups including CISO forum, ISACs, media, schools.

- In support of the recommendation to develop a Cyber 311 Pilot in Austin, CISA should develop a communications plan to amplify the Austin-University of Texas efforts to other cities. This will engage more cities in this initiative and raise awareness of this important work.

- CISA should build out a broader base of support and create new channels for amplifying the agency's key messages.
  - Current and emerging threats such as election interference, mis-, dis-, and mal-information campaigns, network-enabled espionage, ransomware, and IP theft require high levels of response and resiliency across the nation. By building a broader base of support to amplify its cyber hygiene messaging and two-way information sharing with the broadest set of constituents, CISA can increase the nation's resilience to cyber-attacks.
  - CISA should implement the following actions to broaden the agency's base of support for key initiatives:

- Develop a regular cadence of background briefings to cybersecurity reporters.
- Expand the agency's list of validators and create a mechanism to communicate information to validators in real-time. These validators should include individuals and organizations that have broad reach to the American public.
- Capture any messaging (e.g., Shields Up, Russia's invasion of Ukraine, cybersecurity alerts, etc.) and develop narratives to showcase successful messaging campaigns to the public to build trust and confidence in CISA, DHS, and USG writ large.

Conclusion:

CISA has done a tremendous job with stakeholder engagement and public awareness, to date. The outlined recommendations focus on how to amplify key messages, create new programs, and expand reach into a broader audience in order to improve the resiliency of our nation to cyber-attacks.

Acknowledgements:

Members of the SC subcommittee:

Niloo Razi Howe

Ted Schlein

Nicole Perlroth

Mayor Steve Adler

Thank you to the outside experts, CIOs, and CISOs who helped identify the greatest opportunities for increasing resiliency through communication and engagement.