U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

November 28, 2022

MEMORANDUM FOR THE CYBERSECURITY ADVISORY COMMITTEE MEMBERS

FROM: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency (CISA)

SUBJECT: **Formal Response to Recommendations Provided on July 8, 2022**

The Cybersecurity Advisory Committee (CSAC) was established in June 2021 to advise, consult with, and make recommendations to the Cybersecurity and Infrastructure Security Agency (CISA) on the development, refinement, and implementation of policies, programs, planning, and training pertaining to CISA's cybersecurity mission. Since that time, the CSAC has worked to infuse fresh ideas, leveraging its members' significant subject-matter expertise, into CISA's cybersecurity mission.

CISA values the hard work of the CSAC that led to a set of actionable recommendations to improve on CISA's execution of its cybersecurity mission. The expert advice and key insights that the CSAC offers will enhance the work of CISA and keep us well-positioned to help address threats in a rapidly changing cybersecurity landscape.

I have worked closely with my leadership team to determine the feasibility of each recommendation and to ensure that we remain within the legal parameters of CISA's operating authorities and resources. Please find our responses to each top-line recommendation as identified in the enclosure; as you'll see, we've accepted the vast majority of the Committee's recommendations and look forward to implementing them.

Again, I thank the CSAC and its members for their thoughtful recommendations and look forward to continued partnership as we build CISA to be the Cyber Defense Agency our nation deserves.

Enclosure: The Cybersecurity and Infrastructure Security Agency's Response to the Cybersecurity Advisory Committee's Recommendations (Received on July 8, 2022)

CSAC made the following Cyber Hygiene recommendations to the CISA Director:

Recommendation 1: CISA must build out its current Multi-Factor Authentication (MFA) campaign by identifying additional vehicles for publicizing "More than a Password."

Response: Accept. The MFA "More Than A Password" campaign was launched in June 2022 during the RSA Conference. The rollout featured a blog from Director Easterly, a social media blitz with engaging graphics and video-heavy content, as well as a social media toolkit for partners to amplify, a new webpage, a press release that resulted in stories in major trade publications, and this message being featured during our speaking events throughout the conference.

In the months since, CISA has kept the "More Than A Password" campaign going with continued social media content, mentions in major interviews and speaking engagements, and a push with local media.

We gave the campaign another jolt of energy during Cybersecurity Awareness Month. This October, our theme was "See Yourself in Cyber." We engaged new target audiences to see themselves taking action to stay safe online, joining the cyber workforce, and collaborating throughout the industry. Additionally, we will look to build out our public awareness program during Fiscal Year (FY) 2023.

Estimated Completion Date: Ongoing.

Recommendation 2: CISA must take all available steps to ensure that companies working with the federal government fully adopt MFA by 2025.

Response: Accept. CISA will promote full adoption of MFA using the Cyber Performance Goals and Challenges to Industry and by encouraging corporate leaders to take proper cyber hygiene actions.

Estimated Completion Date: Ongoing.

Recommendation 3: Recommend CISA launch a "Cyber 311" campaign to provide an emergency call line and clinics for assistance with cyber incidents for small and medium businesses.

Response: Partially Accept. CISA is partially accepting this recommendation because CISA will consider launching a "Cyber 311" campaign once the outcomes of the University of Texas at Austin's pilot program and any other similar pilots are better understood. This measured approach is consistent with the CSAC's related recommendation that, "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." In the meantime, CISA will leverage its authorities to support local governments that choose to adopt a "Cyber 311" program by providing education, sharing best practices, and identifying available resources.

Estimated Completion Date: Ongoing.

CSAC made the following Mis-, Dis-, and Mal-Information (MDM) recommendations to the CISA Director:

Recommendations 4 and 5: CISA should work to develop metrics for measuring their impact in these efforts. CISA should invest in research to assess the impact of mis- and dis-information and the efficacy of interventions.

Response: Partially Accept. CISA currently leverages output-based metrics such as product downloads from the CISA website, number of engagements, and number of people trained to measure impact. CISA agrees on the importance of developing more robust metrics and a framework to better measure the impact of our efforts and is working to do so. CISA also supports interagency research and development efforts related to risks associated with foreign malign influence operations and disinformation through the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), though we believe that the academic community is likely best positioned to comprehensively study and assess the impact of misinformation and disinformation and the efficacy of resilience-building activities and interventions.

Estimated Completion Date: Ongoing with measures developed in FY 2023.

Recommendation 6: CISA should work to build societal resilience to mis- and dis-information, proactively address anticipated threats, rapidly respond to emergent and persistent informational threats and counter actor-based threats.

Response: Partially Accept. CISA will continue to focus on building national resilience to risks to election infrastructure security associated with foreign malign influence operations and disinformation. In particular, CISA will develop a risk management and resilience-building maturity model, which will help individuals and organizations understand the different components of these risks and how they can best expand their capabilities to be resilient against them.

Within existing authorities, using open source and publicly available research as well as information provided by our interagency partners, CISA will identify, proactively address, and respond to threats of foreign malign influence operations and disinformation that pose risks to election infrastructure. Countering actor-based threats, however, is out of the scope of CISA's mission.

Estimated Completion Date: Ongoing.

Recommendation 7: CISA should focus on addressing mis- and dis-information that undermines critical functions of American society and undermines response to emergencies.

Response: Partially Accept. CISA will continue to develop tools and resources that promote resilience to foreign malign influence operations and disinformation that threatens the integrity of election infrastructure. Given resource constraints, we will remain focused on building resilience to threats specifically to election infrastructure security.

Estimated Completion Date: Ongoing.

Recommendation 8: CISA should assist in creating a "What to Expect on Election Day" plan which would include proactively addressing misleading narratives and creating a workshop for local election officials.

Response: Accept. As with previous cycles, CISA hosted a briefing for media, along with interagency partners and senior election officials, on CISA's and our partners' election security efforts prior to the election to provide awareness of election security activities. The goal was to provide a comprehensive overview of the work CISA, the federal government, state and local election officials, and the private sector have undertaken collectively to ensure the resilience of the 2022 elections. These efforts focused on election beat reporters who were likely to be paying close attention to CISA's work on Election Day, as well as reporters and producers from networks or other major outlets that are not as familiar with our role. This pre-election day briefing was followed by several touchpoints with the media during election day to address any questions around activities related to election infrastructure security.

Estimated Completion Date: Completed.

Recommendation 9: CISA should consider the entire information ecosystem as it makes decisions.

Response: Partially Accept. CISA's ongoing work strives to take into account all major components of the information ecosystem when considering the risks of foreign malign influence operations and disinformation to election infrastructure security.

Estimated Completion Date: Ongoing.

Recommendation 10: CISA should work to detect, warn about and mitigate other threats to critical infrastructure.

Response: Decline. At this time, CISA is not pursuing an ability to independently detect foreign malign influence operations and disinformation that threaten critical infrastructure. CISA receives reporting by the Intelligence Community (IC) on risks to critical infrastructure, including IC reporting on foreign malign influence operations. CISA will continue to warn about and help to mitigate threats to the security of election infrastructure from misinformation and disinformation.

Estimated Completion Date: Not Applicable.

CSAC made the following Strategic Communication recommendations to the CISA Director:

Recommendation 11: Encourage the adoption of MFA through a "More than a Password" partnership campaign.

Response: Accept. See response to Recommendation 1

Recommendation 12: CISA should create a broader base of support and create new channels for amplifying the agency's key messages.

Response: Accept. CISA will continue to accelerate its work building support among stakeholders ultimately helping spread the word on CISA's mission and services. CISA will leverage its ongoing social media and earned media channels as well as expand its stakeholder outreach and speaking platforms to reach new audiences particularly in underserved, target rich, resource poor sectors like healthcare, education, and water.

In addition to these existing channels, CISA will embark on an Awareness and Outreach public awareness program during FY 2023 that will include the development of a new evergreen cyber awareness program. This program will include branding, new partnerships, social media, and earned media.

Cascading from CISA's Strategic Plan that was announced in September, CISA released its Stakeholder Engagement Strategic Plan in October, which will guide the agency in a unified manner in how and why it is engaging across various industry and partner organizations, as well as capturing feedback and metrics to help better inform future engagements, thus creating a broader base of support and new channels for amplifying the agency's key messages.

Estimated Completion Date: Ongoing.

Recommendation 13: Develop a communication plan to amplify the University of Texas at Austin Cyber Pilot 311 program efforts to other cities.

Response: Partially Accept. CISA is partially accepting this recommendation. CISA's goal would be to promote the broader Cyber 311 concept and model if the idea is proven to have impact and value. In furtherance of that objective, CISA can assist with the development of communications plans and strategies available for other cities that wish to establish such a program. CISA can develop a general announcement and launch plan to help these cities publicize this new service and how CISA, as the nation's cyber defense agency, is an available resource. CISA would coordinate this effort with appropriate local officials, as well as any sponsoring entity of the 311 program, and, where CISA drafts any materials, would ensure that CISA's role in drafting is clearly noted.

Estimated Completion Date: Ongoing.

CSAC made the following Technical Advisory Council (Vulnerability Disclosure) recommendations to the CISA Director:

Recommendations 14: Simplify the reporting process and provide feedback to those reporting.

Response: Accept. To ensure security researchers have visibility into the triage status of reported vulnerabilities, CISA will continue to invest in the establishment of a global platform for coordinated vulnerability disclosure (CVD), such as the Vulnerability Information and Coordination Environment (VINCE). VINCE is a shared, web-based reporting and coordination platform which can be utilized by both the researcher and vendor communities to support CVD. The VINCE source code is open, enabling further development and broad implementation across stakeholders.

Estimated Completion Date: Ongoing.

Recommendation 15: Improving security research among groups who will submit vulnerabilities affecting critical systems.

Response: Accept. CISA will pursue the following actions to support the vulnerability research community:

1. CISA will draft and consider implementing a plan to incentivize and support good faith researchers.
2. CISA will examine ways to recognize top researchers.
3. CISA will examine the feasibility of establishing a vulnerability response fellowship.
4. CISA will consider developing a program through which researchers can conduct vulnerability testing on vendor partners' products in a CISA-hosted, widely accessible test range. The result of this testing would be publicly disclosed through CISA's CVD process.
5. CISA will assess opportunities to work with Congress and the Department of Justice to reduce legal liabilities for those wishing to report vulnerabilities in good faith, such as Digital Millennium Copyright Act exceptions for security research.
6. CISA, when prudent, will encourage the use of RFC 9116, which describes how to create a security.txt file in a standardized way to inform security researchers of how to report a vulnerability.

Estimated Completion Date: Ongoing.

Recommendation 16 and 17: Improve the notification processes after a disclosure has been verified and acted on. Enable a frustration-free vulnerability research and reporting environment.

Response: Partially Accept. To help standardize the way in which reports are disseminated, in both human and machine-readable formats, CISA will encourage private sector reporting formats by leading by example with machine-readable software initiatives and by publishing best practices. CISA will explore and work toward adopting a machine-readable advisory format to

accompany human-readable advisory information. CISA's adoption of machine-readable advisory information may encourage private sector adoption.

To link vulnerability information with threat reporting, when applicable and when resourced, CISA will connect disclosed vulnerabilities to the existing ATT&CK or similar frameworks.

To ensure that vulnerability information is easily searchable and can be sorted by make, model, brand, versions, and impacted sectors, CISA will encourage the MITRE Corporation and the National Institute of Standards and Technology (NIST) to enable this functionality within the National Vulnerability Database (NVD), CVE Records, and other databases. However, MITRE and NIST are reliant on information reported to them by researchers, vendors, and private sector organizations to fill these database entries. CISA cannot dictate what the private sector reports to the CVE and NVD programs, which may limit the number of fields within a vulnerability entry that can be parsed for searching.

Estimated Completion Date: Ongoing.

Recommendation 18: Invest in a central platform which will facilitate the intake of suspect vulnerabilities and communication between security researchers, agencies, and vendors.

Response: Accept. CISA will continue to invest in the establishment of VINCE, a software environment open to the community that supports the reporting of vulnerabilities and CVD. The software establishing VINCE is open source, enabling broad implementation across stakeholders.

Estimated Completion Date: September 30, 2023.

CSAC made the following Technical Advisory Council (Cyber Threat Intel) recommendations to the CISA Director:

Recommendation 19: Invest in enriching threat intelligence reports to be more applicable across the three key layers of defense.

Response: Accept. Overall, advancing the useability and impact of Cyber Threat Intelligence (CTI) is a top priority for CISA. For example, the recent improvements made to the Automated Indicator Sharing (AIS) service include improving indicator context and adding a CISA-generated opinion score. In addition, CISA is advancing CTI by developing and testing "low-regret"[1] CTI feeds and creating CTI based on standards derived from detectable adversarial behavior.

Expanding CTI usability to better support stakeholder protection and response capabilities should also be a top priority moving forward. This shift will not only make CTI more useful to the organizations that use it, but it will also increase CTI's overall value, attracting current and new stakeholders to invest more in CTI services, infrastructure, and capabilities. However, to

1. Low-Regret: Taking automated action against this intelligence is extremely unlikely to disrupt operations, regardless of whether or not the intelligence assessment is correct.

truly be successful in expanding CTI's impact, CISA must work to address the systemic stakeholder capacity issues. The impact of quality CTI is significantly reduced if recipients lack the capabilities to put it to use. Being able to build stakeholder capacity through effective and efficient use of CTI is a principal component of the planned suite of CTI shared services that CISA may offer through CISA's Cybersecurity Shared Services Office (CSSO) in the near future.

Estimated Completion Date: Ongoing, expected mid-FY 2023.

Recommendation 20: Explore techniques to enable scalable and effective development of expertise in CTI.

Response: Accept. There is a critical need for not only CTI tools, capabilities, and services, but also support to stakeholders to build their own capacity as experts in the area of CTI. The development and distribution of supporting educational materials (e.g., guidance, training) surrounding the effective generation, consumption, and use of CTI in defensive operations will allow stakeholders to build their capacity and scale across their operations. These materials will need to be developed by CISA's Cybersecurity Services Center of Excellence and Cyber Defense Education and Training group to help ensure that the developed materials follow best and proven practices, are of the highest quality, and are synchronized with existing and proposed efforts to enhance the current and future cybersecurity workforce.

Estimated Completion Date: Ongoing, expected early to mid-FY 2024.

Recommendation 21: Develop and distribute a common open-source stack available to all.

Response: Partially Accept. CISA will collaborate with DHS S&T to develop a set of cybersecurity capabilities that will, when developed, allow for low-cyber-maturity entities to capture, share, and utilize CTI. It will be critical to provide supporting educational materials to decrease the baseline for effective use and implementation.

Estimated Completion Date: Ongoing, expected mid-FY 2024.

Recommendation 22: Invest in a program to make "threat intelligence as a service" available to all qualified users.

Response: Partially Accept. CISA is developing an updated, integrated, and scalable suite of CTI shared services, known as Threat Intelligence Enterprise Services (TIES), which will prioritize a CTI Exchange Platform and CTI as a Service, in addition to updating and modernizing existing CTI services like AIS and Shared Cybersecurity Services. CISA has already initiated a human-centered design process for TIES, and the minimum viable product is expected in late FY 2023 or early FY 2024.

Estimated Completion Date: Ongoing, expected FY 2023.

CSAC made the following Transforming the Cyber Workforce recommendations to the CISA Director:

Recommendation 23: Improve CISA's ability to recruit talent in the cyber workforce.

Response: Accept. CISA concurs with the CSAC regarding the importance of prioritizing strategic workforce development, and just recently, brought on board our first Chief People Officer, as recommended by the Committee, to advance a holistic talent management ecosystem and a people-first culture that will enable us to attract and retain world-class cyber talent. Separately, we have already begun educating hiring officials on cyber recruitment strategies, the authorities that govern our hiring process, and the flexibilities available to us. To maximize our potential candidate pool, CISA leverages LinkedIn, Clearance Jobs, and Dice as social platforms for promoting CISA cyber opportunities. Increasingly, the Handshake social media platform is also used to interact with the student-based population across the nation.

We also concur with the CSAC's recommendation that we need to dramatically improve hiring goals and processes. We are currently looking at ways to streamline our hiring procedures to reduce the time from when a candidate receives an offer letter to when they on-board. However, the goal that CSAC recommends of 90 days from offer to onboarding for cybersecurity candidates may not be attainable given the fact that on average, a security clearance takes 90 to 120 days to complete. We are also unable to move away entirely from a job classification system as CSAC recommends, but we are looking at how to streamline hiring across programs and to significantly expand the use of the DHS Cyber Talent Management System across the agency.

For FY 2023, CISA hiring managers will collaborate with the Office of the Chief Human Capital Officer (OCHCO), the Office of Equity, Diversity, Inclusion, and Accessibility (OEDIA), and the Chief People Officer (CPO) to identify areas of potential underrepresentation within the respective division or mission enabling office (office). The agency will strategically support outreach and recruitment from educational institutions with significant student populations from Underserved Communities—such as Historically Black Colleges and Universities (HBCUs), Hispanic-Serving Institutions (HSIs), Tribal Colleges and Universities (TCUs) and Asian American and Pacific Islander Serving Institutions (AAPISIs), Gallaudet University, etc.—through all recruitment means including but not limited to institution-led job fairs. In addition, hiring managers are encouraged to collaborate with OCHCO, OEDIA, and the CPO to identify opportunities to pursue candidates from non-traditional educational backgrounds/institutions to potentially include community colleges, trade schools, diversity-focused job boards and recruitment agencies, IT/coding programs/bootcamps, diverse professional organizations, as well as those coming from various reskilling or upskilling programs and neurodiverse talent pool initiatives.

For FY 2023, divisions and offices will be asked to assign a subject-matter expert (SME) designee from each subdivision to actively participate in CISA-hosted hiring fairs. Hiring managers are also encouraged to publicize CISA hiring events and employment opportunities on social media such as LinkedIn using standardized language. To the maximum extent practicable, hiring managers should leverage personal and professional networks to direct potential candidates from Underserved Communities toward hiring entry points.

Divisions and offices will designate a SME to participate in at least one Targeted Outreach Activity semiannually at an educational institution or professional organization with significant student populations from Underserved Communities.

CISA currently works with federal partners on two national cybersecurity workforce development programs: the National Centers of Academic Excellence in Cybersecurity (NCAE-C) with the National Security Agency and the Federal Bureau of Investigation; and the CyberCorps: Scholarship for Service (SFS) program with the National Science Foundation and the Office of Personnel Management. There are 384 CAE-C-designated institutions, with more being added each day, and 90 active SFS-participating institutions. Both programs aim to increase the number of qualified professionals entering cybersecurity careers. The NCAE-C program is focused on the production of qualified professionals entering cybersecurity work in both the public and private sectors. SFS primarily targets increasing the number of qualified cybersecurity professionals entering government service. Efforts in both programs span K-12 and higher education. Additionally, CISA also provides engagement and partnership with schools outside of these programs, including engagements with colleges and universities partnering with DHS.

Estimated Completion Date: Ongoing, expected FY 2023.

Recommendation 24: Improve the talent base of the National Cyber Workforce.

Response: Partially Accept. CISA, in general, concurs with the CSAC regarding the importance of improving the talent base of the National Cyber Workforce. To that end, CISA currently supports the U.S. Cyber Games as a founding sponsor. The U.S. Cyber Games was established to build the technical and soft skills of participants that go on to compete in International Cybersecurity Competition (ICC). Additionally, CISA has also sponsored or participated in several other competitions, including Temple University 's Social Engineering (SE) Competition—one of the few SE competitions outside of DEF CON (one of the world's largest and most notable hacker conventions, held annually since 1993)—and focuses on all degree types, not just those with technical skills. CISA also supported the National Collegiate Cyber Defense Competition.

CISA engages in a variety of activities to support the national cybersecurity workforce, including by supporting the newly established NCAE Cyber Games, which will focus on getting more students into cybersecurity through gaming/competition. More broadly, CISA works to expand the availability of cybersecurity education at every level: for the K-12 community through our Cyber Education and Training Assistance Program grant, with higher education institutions through our leadership role in the National Centers for Academic Excellence program, National Cyber League, and collaboration with Historically Black Colleges and Universities and Minority Serving Institutions, and reskilling of the national workforce through our partnership with organizations like NPower, which creates pathways to economic prosperity by launching digital careers for military veterans and young adults from underserved communities, and the President's Cup cybersecurity competition. CISA is continuously exploring other avenues to get

more students and reskilling/retooling professionals interested in cyber through sponsorship of competitions at events like BlackHat, DEF CON, and Women in Cybersecurity.

CISA requested additional personnel and funding in FY 2023 to further relationship building with Minority Serving Institutions (MSI) of higher education and HBCUs. Part of the funding will help CISA to establish the CISA National Learning Consortium, a multi-institutional, cross-disciplinary community with members representing the full spectrum of stakeholders involved in workforce development in cybersecurity, critical infrastructure, and emergency communications. The consortium will work among academia, government, and industry partners to foster access to degree programs that focus on the needs of the nation and government and harmonize training and education curricula. This consortium will also facilitate a cyber educator and cyber expert exchange, responding to developing education and training needs to increase the pipeline of highly skilled cybersecurity, infrastructure, and emergency communications professionals across the public and private domains.

Finally, to improve the talent base of the National Cyber Workforce, the CSAC also recommends CISA establish a virtual Cyber Academy (e.g., a "West Point for Cyber") with a CISA cadet track. The proposal raises significant programmatic resource concerns that would require evaluation and clarification of practicable implementation options that are consistent with CISA's existing authorities and funding. While some virtual Cyber Academy operational options may require additional Congressional authorization and/or funding to implement the recommendation, CISA presently provides cybersecurity training to individuals across the country through programs like the Federal Virtual Training Environment, which is available to federal, state, local, tribal, and territorial government employees, federal contractors, and U.S. military veterans, and specialized technical training on topics such as Industrial Control Systems cybersecurity.

Estimated Completion Date: Ongoing, expected FY 2023.