U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

October 31, 2016

Via FEMA-NCIRP-engagement@fema.dhs.gov

Andy Ozment
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Dear Assistant Secretary Ozment:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, welcomes the opportunity to comment on the draft National Cyber Incident Response Plan (NCIRP).

The Chamber was pleased to host the administration's release of Presidential Policy Directive-41, United States Cyber Incident Coordination (PPD-41).[1] While our organization was not directly involved in writing the revised National Cyber Incident Response Plan (NCIRP), we generally believe that the draft, which was only released publicly on September 30, is a workable start.[2] We appreciate the time and effort that both government and industry officials devoted to writing the draft document. This letter highlights constructive elements of the proposed NCIRP and recommends areas for improvement.

POSITIVE COMPONENTS OF THE NCIRP

- **Clarification of federal roles and points of contact.** The NCIRP notes, consistent with PPD-41, that (1) the FBI will take the lead in coordinating the response to the threat; (2) the Department of Homeland Security (DHS) will take the lead in coordinating asset response, such as helping organizations deal with the impact of a cyberattack and preventing the attack from spreading to other information systems; (3) and the Office of the Director of National Intelligence's (ODNI's) Cyber Threat Intelligence Integration Center (CTIIC) will take the lead in integrating intelligence and analysis about the threat and identifying opportunities to mitigate and disrupt it.[3]

The NCIRP, especially Annex C, responds to calls from the private sector to provide clarity and guidance about a central question, "Who do I call to report cyber incidents and get help?" (NCIRP, pg. 37). Many companies and associations have relationships with government authorities in bodies such as the FBI, DHS, and the Secret Service. Yet many private organizations do not, so key federal points of contact are useful.[4]

- **Involvement of the private sector.** The NCIRP puts forward a common homeland security principle that cybersecurity is a "shared responsibility," namely that the private sector and government agencies have complementary responsibilities to protect the United States from malicious cyber activity and manage cyber incidents (NCIRP, pg. 2).

  The NCIRP says, "The private sector, especially the owners and operators of critical infrastructure, plays a key role in responding to cyber incidents. Small, medium, and large private sector entities are often the first and primary responders to cyber incidents." The draft goes on to point out, "Private companies are responsible for the security of their own systems, and they are normally the first to identify an incident and are often in the best place to respond to it" (NCIRP, pg. 7). Still, in the Chamber's experience, businesses may require more timely and substantive assistance from government, which we address here.

- **Inclusion of a cyber schema provides a useful visual aid.** Annex B of the NCIRP features a Cyber Incident Severity Schema (the cyber schema), which describes the intensity of cyber incidents affecting the nation. The cyber schema establishes a frame of reference for evaluating and assessing cyber incidents along the following lines of inquiry: (1) the severity of a given incident, (2) the urgency required for responding to a given incident, (3) the seniority level necessary for coordinating response efforts, and (4) the level of investment required of response efforts (NCIRP, pg. 36).

RECOMMENDATIONS TO IMPROVE THE NCIRP

- **Remove reference to certifying information-sharing and analysis organizations (ISAOs).** The NCIRP references Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, and notes that DHS is "facilitating efforts to identify procedures to create and *accredit* [italics added]" or certify ISAOs (NCIRP, pg. 25). The Chamber suggests removing the reference to "accredit." Deleting "and accredit" on line 1045 would not interfere with the meaning of the sentence.

  Moreover, the ISAO Standard Organization (ISAO SO), which was tasked with developing standards for ISAOs, released an initial set of voluntary guidelines on September 30. The group intentionally did not include language on "minimum requirements" or the role of "certification" for ISAOs.[5] The Chamber has communicated to both DHS and ISAO SO principals that it is too early in the process to certify and set minimum requirements for ISAOs.[6] Many in industry contend that mandates would restrict, not enhance, the growth of information-sharing bodies.

- **Promote the cybersecurity information-sharing law.** Most policy and business observers agree that effective cybersecurity information sharing is an important method of protecting organizations' networks and responding to incidents. President Obama signed the Cybersecurity Information Sharing Act of 2015 (CISA) into law in December 2015, which the Chamber applauds. The new law is meant to spur protected, automated sharing. The NCIRP lists the Cybersecurity Act of 2015 (P.L. 114-113), of which CISA is a part, in Annex A (NCIRP, pg. 34). However, CISA, protected information sharing, and the DHS-administered Automated Information System (AIS) are not listed, but they should be to promote the tools they offer private organizations.[7]

- **Tighten public-private response coordination.** The NCIRP suggests a level of standoffishness between industry and government that may not work for many companies and sectors. According to the NCIRP, federal entities "typically will not play a role" in a business' response activities, but authorities will "remain cognizant" of the entity's response efforts (NCIRP, pg. 12). We recognize that cyberattacks cannot be handled solely by government. Yet cyberspace is the only domain where the government asks private companies to defend themselves against foreign powers and other significant threats, which is unworkable in many instances.[8]

  Indeed, government does not stand between private entities and malicious hackers. Some companies want to forge closer working relationships with government agencies. Federal officials should facilitate such partnerships and knock down any policy and legal hurdles.[9] At the same time, the converse should hold true. Some in industry may want to keep government entities at arm's length for myriad reasons. Such a position should be respected.

- **Explain how the cyber schema works by regularly using it.** The next administration will need to create greater fluency among stakeholders regarding the cyber schema. The severity levels seem feasible to the Chamber, but what's needed is a better understanding—via some showing and telling—of where cyber incidents fit on the five-part architecture. Essentially no policymaker or business official that the Chamber speaks with can pinpoint where a cyberattack would fit along the continuum—ranging from least severe (level 0/baseline/white) to most severe (level 5/emergency/black)—with precision. Three high-profile cases are worth pondering in terms of how the cyber schema may work in practice:

  - In 2014, a grand jury in the Western District of Pennsylvania indicted five Chinese military hackers for computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries.[10] Where would these cases line up on the cyber schema?

  - This past March, several Iranians were indicted for a series of cybercrimes that cost U.S. financial institutions tens of millions of dollars and compromised critical controls of a New York dam.[11] Where would these episodes appear on the cyber schema, if at all?

- Earlier in October, the U.S. intelligence community said it was "confident" that the Russian government directed the recent compromises of emails belonging to American individuals and political organizations.[12] The administration's public declaration shows that U.S. officials view the hacking as having a qualitative and/or quantitative impact on our economic and national security. Thus, would the cyber schema apply, and how?

Perhaps the administration is using the cyber schema internally and discreetly, which is understandable. However, if the NCIRP is to be useful in the real world and not just a paperwork exercise, the next administration will need to select incidents, explain its decision making regarding the severity of the incidents, and indicate where they line up on the cyber schema.

In the Chamber's view, if the NCIRP is going to be meaningful, the cyber schema needs to be used regularly. After all, businesses rely on certainty to help make optimal decisions and marshal their resources. In the context of responding to a cyber incident, expectations for future actions are rooted in concrete experiences and intuition—having an expert feel for how a cyber incident may stack up on the cyber schema and what activities likely need to follow. Individuals in industry and government won't amass valuable expertise if the cyber schema is not used fairly frequently.[13]

Here's an idea for gradually moving forward. Top federal officials may not want to make declarations publicly available right away. ("The OPM breach is a level 3 or 4 incident," for example.) But they could vet their initial thinking with trusted industry partners, particularly sector-coordinating councils, associations, and leading companies so that there is a common understanding and predictability about future announcements.

- **Connect the NCIRP to a national cybersecurity strategy.** It's unclear where the NCIRP fits in the U.S. government's overarching cybersecurity strategy, which is still needed. Despite the existence of written blueprints, the U.S. cybersecurity strategy is seemingly uncertain, both to many in the private sector and our adversaries.

  Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence, which is roughly equivalent to improving U.S. defenses and imposing costs on bad actors. Arguably, a key goal of responding to a national cyber incident is reducing the benefits of conducting harmful cyber activity against the business community and the country's interests. The upcoming administration should engage the private sector and other stakeholders on connecting the NCIRP to cyber defense and deterrence. The pros and cons of cyber response and deterrence deserve more careful scrutiny than they have received to date.[14]

  The Chamber believes that there is untapped capacity among parties in the government and private sectors that needs to be put to greater use, exercised, and redeployed to check cyber incidents before they happen.

***

The Chamber appreciates the opportunity to offer our views to DHS concerning the draft NCIRP. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com; 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Notes

[1] www.c-span.org/video/?413604-1/federal-officials-discuss-cybersecurity, www.uschamber.com/above-the-fold/government-business-staying-step-put-out-cyber-fires

[2] www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment

[3] www.whitehouse.gov/the-press-office/2016/07/26/remarks-aphsct-lisa-o-monaco-international-conference-cyber-security

[4] www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf

[5] www.isao.org/news-updates/isao-so-releases-initial-voluntary-guidelines

[6] http://insidecybersecurity.com/daily-news/creating-trust-through-certification-cyber-info-sharing-remains-open-question, http://insidecybersecurity.com/daily-news/isao-standards-group-sidesteps-minimum-requirements-its-upcoming-guidance

[7] www.us-cert.gov/ais

[8] www.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us

[9] www.defenseone.com/technology/2016/10/us-needs-one-cyber-defense-agencynot-three-top-nsa-official-says/132474/?oref=d-river&&&utm_term=Editorial%20-%20Early%20Bird%20Brief

[10] www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[11] www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector

[12] www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement

[13] www.scientificamerican.com/article/kahneman-excerpt-thinking-fast-and-slow, www.youtube.com/watch?v=CjVQJdIrDJ0

[14] www.nist.gov/sites/default/files/documents/2016/09/15/coc_rfi_response.pdf