February 5, 2020

To the Department of Homeland Security,

The Cybercrime Support Network (CSN) began in 2017 as an organization dedicated to meeting the challenges faced by millions of individuals and businesses affected each and every day by cybercrime. In that time, we have worked to build reporting structures at the state and local level for individuals and small-to-medium businesses (SMBs) which face data breaches, online fraud, identity theft, and other forms of cyber incidents. Today, CSN is actively partnered with 211 Call centers in six states, and we anticipate an additional 3-5 state level partnerships by the end of 2020. Our victims' resource website, Fraudsupport.org, has received 658,530 unique hits since its creation, and CSN is frequently developing and distributing resources for individuals in the form of videos, blog posts, educational explainers, and other online content to serve victims.

In September 2019 CSN signed a cooperative agreement with the Department of Homeland Security (DHS) Cyber and Infrastructure Security Agency (CISA) to build on this work, and to establish a State, Local, Tribal, and Territorial (SLTT) Cyber Reporting and Threat Information Sharing Pilot related to consumer and small-to-medium (SMB) cyber incidents. For this Pilot, CSN will help DHS CISA to achieve eight specific objectives, which all broadly fall into three main lines of effort: 1) Standardizing cyber incident reporting; 2) Curating resources for response and recovery, and 3) Developing Information Sharing Processes.

In short, CSN is a front-line leader on issues around cyber incident reporting.

With this in mind, we write to provide comments on DHS CISA's potential changes to its online cyber incident reporting forms for critical infrastructure. Though distinct, our focus on ***individuals and SMBs affected by cyber incidents*** nonetheless provides useful lessons for your consideration. Broadly, we appreciate efforts to improve such reporting, and thank the Department for making an effort to update these forms. Specifically, however, we write to provide helpful guidance for consideration as you move forward in considering and implementing further changes.

1. Still in the early stages of the SLTT Cyber Reporting and Threat Information Sharing Pilot mentioned above, CSN has wrestled with critical questions identified by the Office of Management and Budget (OMB) as those it is

"particularly interested in".[1] Indeed, both in the development of our training materials for our 211 partners and in the build out of a national-level reporting form, CSN is *also* faced with understanding the "practical utility" of information collected in such a reporting form and desire to "minimize the burden of the collection of information".

a. Partnering with the Mississippi State University National Strategic Planning & Analysis Research Center (NSPARC), CSN is designing an online reporting form for individuals and SMBs to report cyber incidents. This form builds on and echoes the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reporting form. In particular, CSN's form is intended to:

i. Integrate with 211 human services organizations and processes to further enhance accessibility and to provide other "human services" that victims might need;

ii. Incorporate stronger usability standards;

iii. Integrate more fully with other investigative organizations at the SLTT level and across government for enhanced sharing of incident reports; and

iv. Integrate more fully with preventive organizations at the SLTT level and across government and the private sector for enhanced sharing of threat information.

b. Only three months into the ongoing SLTT Cyber Reporting and Threat Information Sharing Pilot, CSN has already identified a number of existing efforts which can inform cyber incident reporting forms. For example, the Aspen Institute's Tech Policy Hub has produced a useful instructional briefing, entitled "Protecting Seniors Via Technology & Design Policy". This offers insight into how to design online reporting forms which senior citizens can use effectively.

CSN has incorporated lessons from this brief into our own work. We strongly recommend that such existing efforts be considered and reviewed as you work to improve cyber incident reporting forms for critical infrastructure.

2. As a recognized leader in the field of cyber incident reporting engaged in a pilot effort to study the feasibility of a national cyber incident reporting system for individuals and SMBs, CSN and its partners stand ready to support DHS CISA and provide lessons-learned from our effort which can be applied to your review of cyber incident reporting for critical infrastructure. Indeed, it has become increasingly clear in recent years that emerging and persistent threats to cybersecurity cannot be neatly separated — often a malicious actor(s) will apply tools and tactics in one field to another. As the Department's own Cybersecurity Strategy, released in May 2018, makes clear:

[1] Department of Homeland Security, "CISA Reporting Forms," The Federal Register, Vol. 85, No. 3, January 6, 2020.

The broad availability, relatively low cost, and increasing capabilities of cyber tools also affect trends in the threats we face… Malicious cyber tools sold on the Internet can be adapted to intrude into systems and otherwise commit criminal acts related to financial fraud, money laundering, intellectual property theft, or other illicit activities.[2]

The rapid evolution of the cyber threats we face – as individuals, businesses, infrastructure, and governments – requires similarly adaptive and effective collaboration in response. For this reason, CSN writes to add:

a. It is critical that DHS and all Federal, State, Local, Tribal, Territorial and Private Sector Partners work together in a wholistic fashion to refine cyber incident reporting and information sharing systems. Please consider how changes made to the cyber incident reporting forms for critical infrastructure can complement other cyber incident reporting efforts.

b. Extending the public comment period for this effort was a valuable step in gathering useful perspective from a wide array of communities of interest. Going forward, please consider how to directly engage those outside of the Federal government, whether civil society such as CSN or SLTT level agencies and the private sector, to continue to incorporate their insight into your efforts.

c. Finally, please consider publicly sharing your lessons learned from the evolution of your incident reporting forms for critical infrastructure with communities of interest. This will be a valuable contribution to organizations like CSN which are leading the way on similar efforts in other areas.

CSN is grateful for the opportunity to provide comment on the potential changes to your cyber incident reporting forms. We remain committed to our mission of supporting those individuals and SMBs affected by cyber incidents and ensuring that reporting mechanisms are effective is a key part of that objective. Because of this, we are ready to provide any further assistance in your effort.

If you have any further questions or concerns, please contact Mr. Alan Carroll, Senior Director for Engagement and Strategy, at alanc@cybercrimesupport.org.

Sincerely,

Kristin Judge

Kristin Judge,
Founder and Chief Executive Officer
Cybercrime Support Network

[2] US Department of Homeland Security, "U.S. Department of Homeland Security Cybersecurity Strategy", May 15, 2018