

Testimony of Dr. Gregory E. Shannon
Chief Scientist for the CERT Program at
The Software Engineering Institute at Carnegie Mellon University
House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
“Hearing on Draft Legislative Proposal on Cybersecurity”
December 6, 2011

Chairman Lungren, Ranking Member Clarke, and other distinguished members of the subcommittee, thank you for the opportunity to testify; it is my pleasure to discuss your draft legislation.

About CERT®

The CERT Program is part of the Carnegie Mellon University Software Engineering Institute (SEI), a Department of Defense federally funded research and development center (FFRDC) located on the Carnegie Mellon campus in Pittsburgh, Pennsylvania (www.sei.cmu.edu).

The CERT Program (www.cert.org) has evolved from the first computer emergency response team, created by the SEI at the request of the Defense Advanced Research Projects Agency (DARPA), in 1988 as a direct response to the Morris worm incident. The CERT Program continues to research, develop, and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works both to mitigate cyber risks and to facilitate local, national, and international cyber incident responses. Over the past 23 years, CERT has led efforts to establish over 200 computer security incident response teams (CSIRTs) around the world – including the Department of Homeland Security (DHS) US-CERT. We have a proven track record of success in transitioning research and technology to those who can implement it on a national scale.

I am Dr. Greg Shannon, the Chief Scientist for the CERT Program, where I lead efforts to sustain and broaden CERT’s strategic research, development and policy initiatives.

Testimony

I first want to ensure that the committee appreciates the exceptional work that is under way at the Department of Homeland Security (DHS) in the area of information sharing. I understand frustrations with the current range and pace of information sharing, but I assure you that DHS is making great progress. The type of information that organizations are being asked to share with each other and the U.S. government is sensitive, and sharing such information requires trusted relationships, established and tested over time. Established trust is a key success factor for such programs, and reliable trust takes time.

Working from the objectives of the current draft legislation, drawing on CERT's 23 years of experience, and using concepts from public health models¹, I will discuss how to leverage current efforts, the strengths and challenges of both the current efforts and the legislation, and specific recommendations. The mission of our FFRDC is to improve the state of the practice, so I will focus on what should be done versus who should be doing it.

I endorse the committee's proposal to position a non-profit private entity to serve as a national clearinghouse for the exchange of cyber threat information – the NISO (National Information Sharing Organization). We believe that a “third-party, honest broker” facilitator for the disclosure and dissemination of cyber-security intelligence creates a superior and more productive environment where all participants, both government and non-government, more readily share sensitive information. Moreover, it is imperative that the designated organization is making decisions for the greater good based on the highest quality data, openly acquired and objectively analyzed.

Many of the goals proposed for the NISO have parallels to the activities of the Centers for Disease Control and Prevention (CDC) – the fact that it is a federal agency notwithstanding. As the nation's leader in health, monitoring, prevention, and preparedness, the CDC works to monitor and prevent outbreaks, implement prevention strategies, and maintain national statistics – it is a central clearinghouse for information with response capabilities. Crucially, it does so by working with partners throughout the nation and the world to collaboratively create the expertise, information, and tools that people and communities need to protect themselves.

We envision the NISO, like the CDC, filling a cyber information leadership role while interacting with existing groups. The NISO, run by a non-profit would have in-house functions, maintain a common operating picture, and the 24/7 help desk, but its biggest role will be to interface with present day efforts and improve communications and collaboration. I want to ensure the committee recognizes the ongoing work within established frameworks and discuss the benefits of utilizing progress already made. To add yet another institution could in practice derail the current advancements and delay the committee's ultimate goal of timely information sharing. I suggest that instead of creating a duplicative organization, the committee charge the NISO with being the single point of interaction for those successful efforts and, when appropriate, consolidate work under the NISO.

I share and understand frustration that capabilities for cyber threat information sharing are not being created quickly enough. Human nature reasons that adding people to a late or slow project will accelerate performance; however, Brooks's Law, also known as the “mythical man-month,” suggests otherwise. Based on his experiences at IBM, Dr. Fred Brooks states: “adding manpower to a late software project makes it later².” Brooks found that there is “ramp up” time to adding staff to a project – they aren't productive immediately, and their education diverts resources from the rest of the team. Furthermore, a new player sharply increases communication

¹ I am drawing on ideas and language in the forthcoming report from the EastWest Institute, *Using a Public Health Model to Support Collective Action to Improve Global Internet Health*, that is being written by an international private-sector-led working group.

² Frederick P. Brooks, Jr. "[The Mythical Man-Month](#)." 1995 [1975]. Addison-Wesley.

costs. As you add additional “reporting” bodies, confusion as to who should be told what and when is only exacerbated. Everyone working on the same task needs stay synchronized, so as more people are added, they spend more time trying to find out what everyone else is doing. Furthermore, Dr. Brooks famously said, “Nine women can't make a baby in one month,” implying that regardless of the manpower, some undertakings just take time. For information sharing, building the necessary trust relationships cannot be rushed.

To better understand our vision, I have mapped out how a NISO organization might look – see Diagram 1. In doing so, we made assumptions about the overall goals of the organization based on the stated and implied objectives, and I encourage the committee to think carefully about what problems they want the NISO to solve and how the structure and authority of the NISO helps solve those problems. Using CERT’s experience we have listed what we see as the necessary capabilities and enablers for a successful NISO.

There are four critical success factors for such an entity to accomplish the objectives set out: data of value, trust, protections, and policy. First, for the NISO to have success, it absolutely must be able both to share and facilitate the sharing of timely, actionable information. The existence of the former will enable the latter. Furthermore, that which the NISO shares must be distinct and not readily attainable by participating organizations. Otherwise there is little or no incentive to participate. The value of NISO’s information would come from either being the exclusive distributor of an insight through novel aggregations or applying a new analysis technique to unique, participant-shared, or public information. Providing valuable data is not only the result of having access to unique data, but also the ability to fundamentally analyze the data differently to provide real, actionable, intelligence from which best practices are derived. For the NISO to truly serve a significant and useful role, the timely and actionable information they disseminate to participating organizations must be reactive as well as proactive, such as best practices. The promise of exclusive information, such as fused analysis of network data, network traffic, or forensic artifacts, will be the value added that NISO participants need to justify their participation. This information will also differentiate the suggested common operating picture (COP) from the several entities that offer situational awareness, and bring the necessary added value to ensure participant involvement. Furthermore, the COP should strive to be able to fundamentally analyze the data differently, further differentiating the NISO from similar organizations and enticing participation. This function would draw nicely from the anticipated collaborative research and development. Like the CDC, the NISO needs distinctive capabilities that make it the “go-to” organization for cyber threat awareness.

Next, I want to stress to the committee the importance of trust to facilitate meaningful exchanges. The need for trust is yet another reason that building on existing efforts is important. While there may be frustrations with the current range and pace of information sharing, you cannot legislate trust, and any new organization needs time to build the necessary relationships for meaningful communications. I believe the committee’s intentions are best served by building upon the existing rapports.

Lastly, it is imperative that solid protection mechanisms and safe harbors be in place for the designated organization and its participants for unencumbered information sharing and analytical product delivery to occur. This will likely require both legislative updates and policy changes,

which must be done with the utmost care to privacy and civil liberties. This is an important yet difficult task, and I commend the committee for beginning the dialogue.

Moving on to the information sharing objective of the NISO organization: As you can see from Diagram 2³ (NISO relationships with existing efforts), there are currently many organizations that “specialize” in information sharing. Several government agencies have information sharing entities – not just DHS – and not to mention the hundreds of private sector and academic entities, some quasi-government, that all claim to be centers where cyber information can be shared. Without a recognized body, coordinated with United States government (USG) efforts, private sector organizations are confused about with whom and under what circumstances they should engage all of these other efforts. This fragmentation results in sub-optimal dissemination of timely information. NISO would serve as the national cyber-security aggregation point and coordination center endorsed by and coordinating with the federal government. We advocate establishing a single point of interaction, to be run by the designated non-profit entity, while collaborating and working with the mechanisms and organizations already in place. For certain operational tasks, it might make sense to re-brand current efforts and place them under the NISO, all the while ensuring we are building on the successes and not starting over.

For the sake of clarity I will run through a real world example of a cyber threat and how a NISO, organized as suggested above, would have had a positive impact on the situation. Let us take the Conficker worm, first discovered in early November 2008, which used flaws in Microsoft Windows software to infect millions of computers. Realizing a collaborative effort was needed to combat the advanced malware techniques behind Conficker, an industry group was serendipitously formed during an ICANN conference in February 2009. While the Conficker working group (CWG) had many successes, and several similar working groups have since formed using the same model, the threat clearly demonstrated gaps in our national capabilities. First and foremost, the ramp up delay: the effort expended to form the group and time spent finding the right skill sets, capabilities and authorities before any work could be done on the problem at hand. Had there been an established and trusted entity, such as a NISO, Microsoft could have approached them and begun combating the problem much sooner. There are other gaps the CWG has conceded they were unable to fill, such as the need for a dedicated project manager, administrative support, testing facilities, and a more coordinated approach with the anti-malware tool vendors – roles that a NISO could clearly execute. Likewise, there are lessons to be learned from why the group was successful. The CWG has attributed their success to trust. The operational members of the group all knew each other, had previously worked with each other, and had confidence that all members would do a good job, follow through with their given tasks, and do no intentional harm. That trust was the glue that enabled a group of colleagues to form an effective collaboration that was largely able to contain the worm. Their success

³ Caveat: The diagram is in no way truly comprehensive of all the current organizations that claim to be cyber information sharing centers. These are simply some of the most prominent entities. Furthermore the relationships represented in the diagram are derived from public mission statements and budget documents and are meant to be illustrative, not comprehensive.

corroborates the model of a third party organization working with existing functions and building on already established relationships.⁴

I encourage the committee to require that the NISO maintain a national repository of malware for research purposes. Currently there are several organizations that have malware repositories but they are seen as a competitive advantage and rarely shared. Access to such a repository would enable cyber research to reach new levels. Currently researchers work with only small pieces of the puzzle, resulting in reactive research, and impeding research that can look more globally at the problem. Again, if we use the public health model, imagine if cancer researchers were only told that cancer affects thousands of people who die every year, and the data was broken down by neither type nor outcome. Such data would make it impossible to make well informed decisions about priorities for response as well as research. Armed with a well-maintained malware repository, with appropriate controls on access, the NISO could provide more effective methods for basic cyber hygiene.

Finally, I want to touch upon the bill's research and development objectives. Given the preponderance of threats, standards, technologies, products, best practices, etc. in cyber security, I strongly encourage the committee to include language in the legislation that emphasizes the need for *operationally and scientifically sound capabilities*. Not every best practice scales well, and not every technology has scientifically sound evidence of its efficacy *and* its limitations. The academic research community increasingly recognizes the need for such sound methods as evidenced by workshops on Cyber Security Experimentation and Testing (CSET)⁵ and Learning from Authoritative Security Experiment Results (LASER)⁶. Such legislation language would create an important positive demand for well-formed pilots and experiments that produce broadly meaningful data and results. This would stimulate the development and maturation of ever-improving methodologies for pilot projects, assessments, experiments, and research.

For example, in the draft language, phrases such as the following are used:

- Develop and conduct risk assessments
- Comprehensive assessment techniques
- Foster the development of essential information security technologies
- Facilitate the adoption of new cyber security technologies and practices
- Guidelines for making information systems more secure at a fundamental level
- Catalogue of risk-based performance standards
- Cyber security research and development

I recommend adding clarifications that such artifacts and activities are:

- Operationally valid and scalable in situ
- Scientifically, theoretically, and/or experimentally valid or sound
- Evidence-based capabilities and limitations

⁴ Nazario, Jose. "Conficker Working Group Overview." Institute for Information Infrastructure Protection (I3P). 12 October 2011. Web. <http://www.thei3p.org/docs/events/cybercprfiles/NAZARIOI3PCONFICKER.pdf>.

⁵ Established 2008: <http://www.usenix.org/events/cset12/index.html>.

⁶ New: Learning from Authoritative Security Experiment Results (LASER), <http://www.laser-workshop.org>

Participants can further facilitate effective security by authorizing the NISO to support creation of and access to high-fidelity data sets to qualified researchers, of course with appropriate access controls. Access to such data is essential for creating and evaluating critical technologies and best practices, especially to understand important limitations.

To finish, I want to applaud the committee's foresight in combining research functions with operational objectives in the NISO design. It is an ambitious and difficult task, and consequently there are currently few successful mixed organizations. Nevertheless, combining research and operations can and does have many benefits. I see the SEI's CERT Program as a viable model for successfully bringing together research and operations to add value to both communities. At CERT, our strategy is to create usable technologies, apply them to real problems, and amplify their impact by accelerating broad adoption. Having one foot in operations gives us the insight into real-world problems and ensures our research has real-world applications. Moreover, having operational access gives us the opportunity to test our research and make the necessary improvements for a successful and scalable transition.

Thank you for the opportunity to comment on this important legislation and leverage CERT's 23 years of experience in the area of information sharing.

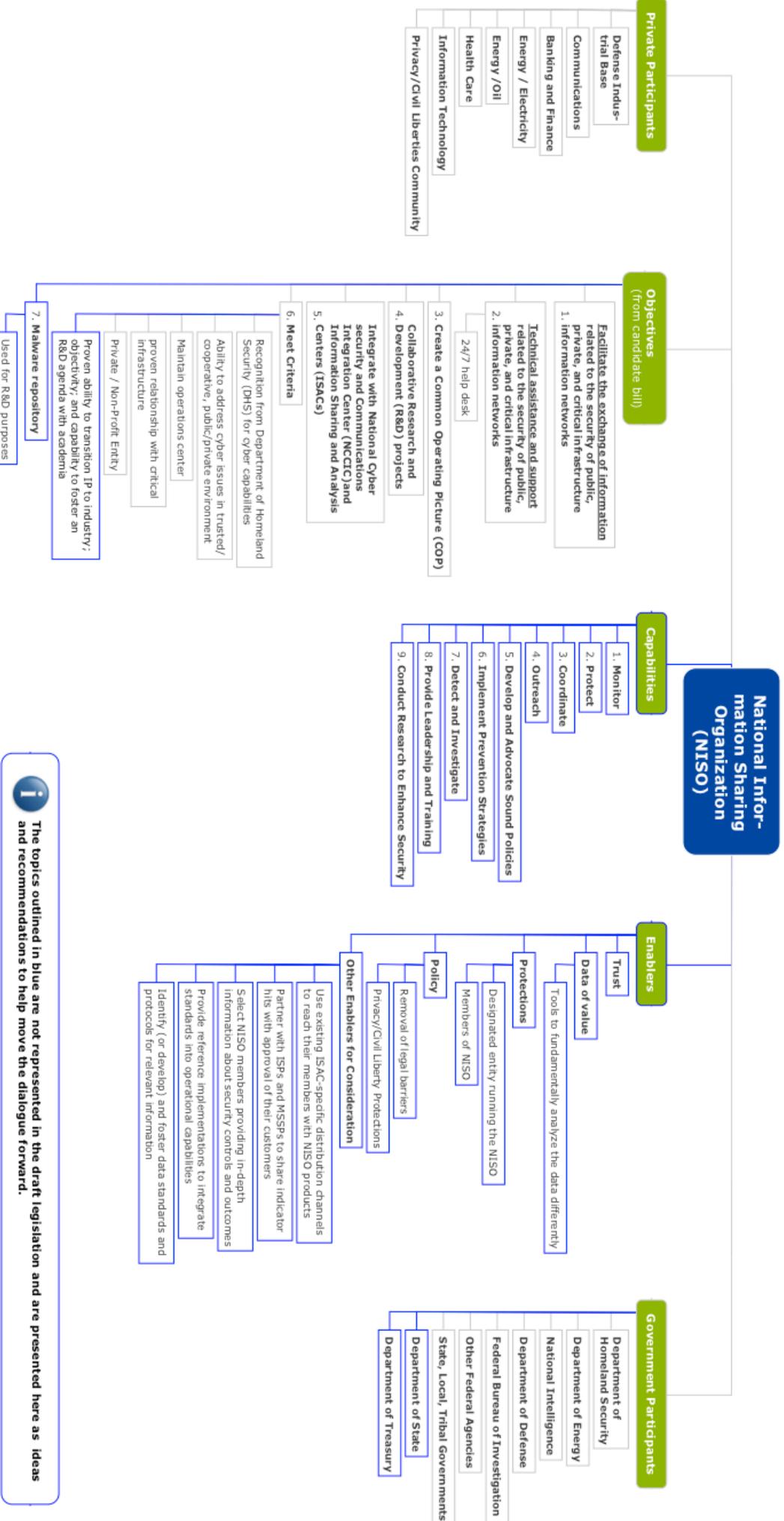
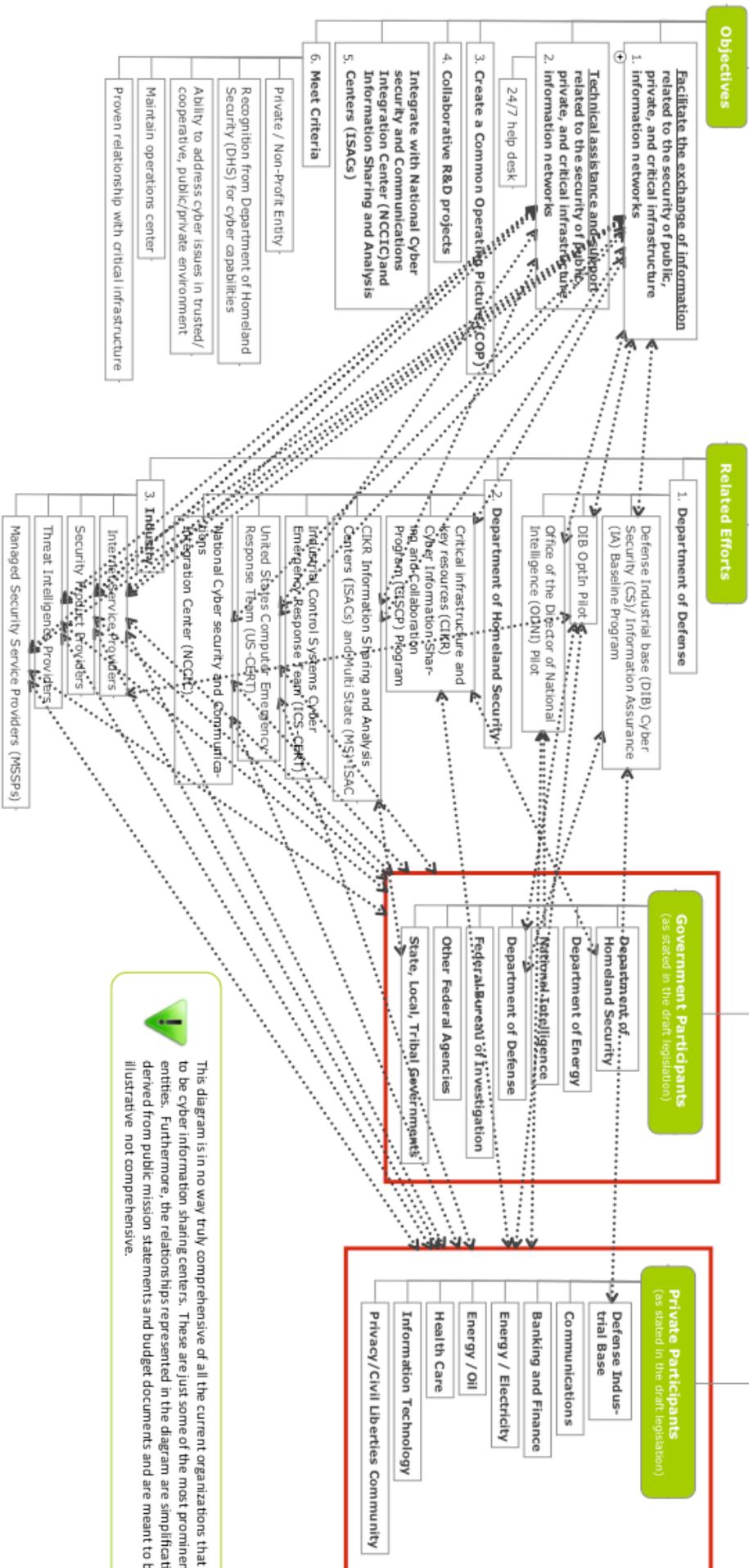


Diagram 1



The Software Engineering Institute (SEI) is a federally funded research and development center, operated by Carnegie Mellon University. The SEI's purpose is to provide technical leadership to advance the practice of software engineering so government organizations and industry may acquire and sustain software-intensive systems with predictable and improved cost, schedule, and quality. This paper is intended only for educational purposes. © 2011 Carnegie Mellon University

National Information Sharing Organization (NISO)



! This diagram is in no way truly comprehensive of all the current organizations that claim to be cyber information sharing centers. These are just some of the most prominent entities. Furthermore, the relationships represented in the diagram are simplifications derived from public mission statements and budget documents and are meant to be illustrative not comprehensive.

Diagram 2

The Software Engineering Institute (SEI) is a federally funded research and development center, operated by Carnegie Mellon University. The SEI's purpose is to provide technical leadership to advance the practice of software engineering so government organizations and industry may acquire and sustain software-intensive systems with predictable and improved cost, schedule, and quality. This paper is intended only for educational purposes. © 2011 Carnegie Mellon University