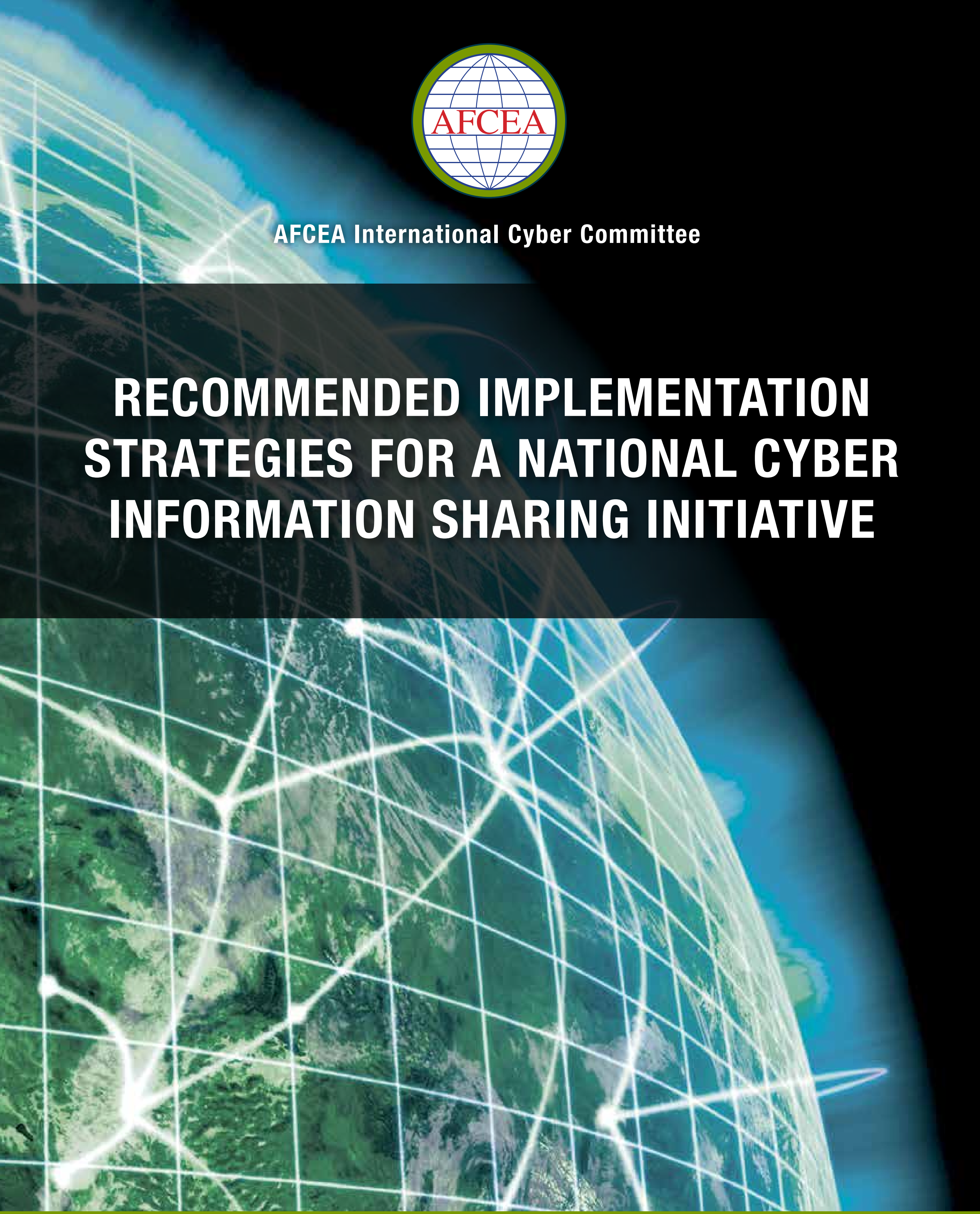
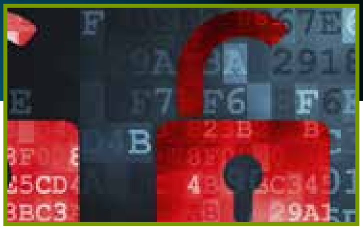


AFCEA International Cyber Committee

RECOMMENDED IMPLEMENTATION STRATEGIES FOR A NATIONAL CYBER INFORMATION SHARING INITIATIVE

April 2016



INTRODUCTION

The AFCEA Cyber Committee has continued to evaluate the appropriate strategies for improving our nation's approaches to information sharing. In the fall of 2014, the committee developed a set of recommendations and provided them to the White House team evaluating this topic. More recently, the committee provided recommendations regarding the appropriate context and framework for developing a national cyber information sharing infrastructure. This paper addresses recommendations for implementation strategies that should be pursued in implementing the provisions of the executive order (EO) on information sharing[1]. However, the committee believes that a successful implementation of the EO requires an appropriate context for these efforts as well as a framework that could be used to define success.

ROLL-OUT OPPORTUNITIES AND IMPLEMENTATION

As implementation continues, the government must specifically enable the outcomes envisioned in the EO and remove potential obstacles, including those described below.

Define standards that the private sector will find useful. A broad-based input into the information sharing standards is essential for success. As the National Institute of Standards and Technology (NIST) Cyber Framework is undergoing revision in parallel, we suggest leveraging the framework working groups to simultaneously engage in the development of ideas and a companion "framework" for information sharing. This will allow those organizations debating enhancements and updates to the NIST Cyber Framework to address the two very interconnected activities simultaneously. This will also avoid duplication of convening industry review groups, making it clear that the two issues are mutually beneficial, and help ensure compatible and complementary language. This approach has the additional benefit of broadening industry participation in both efforts because some communities concern themselves with one over the other; both are critical and could benefit from broader participation.

[1] Executive Order -- Promoting Private Sector Cybersecurity Information Sharing (EO 13691)

Enable (some) of the Information Sharing and Analysis Organizations (ISAOs) to get their feet under them by providing direct, and in some cases, ongoing support from the Department of Homeland Security (DHS). The support needed by the future ISAOs will vary widely and will evolve over time. One thing is common to all current Information Sharing and Analysis Centers (ISACs) — many of which will become ISAOs — no two are alike. This is not by design, but by necessity. What will ultimately work for ISAOs will be a spectrum of approaches and the unique maturity needs of the ISAOs will, by necessity, require varying kinds of support: financial, technical or other types of support. Enabling these will require careful consideration of the relative value to ISAO members, as well as the broader ecosystem they may represent.

Define a clear value proposition to establish, join and stay actively engaged with ISAOs. Organizations may enthusiastically come to the ISAO "table" on day one; but, curiosity, promises, patriotism and fear will only keep people in the room for so long. Organizations will not sustain active participation without seeing immediate value and return on their investment (be it time, money or intellectual capital) in the form of demonstrable enhancements to their individual security position. Understanding what brings each of the ISAO participants in; what sustains them; what they value; and how they can explain it to their organizational decision makers will all be essential success factors.

As government officials have acknowledged, the need for the entities waging this cyber "war" to be able to collaborate and share relevant information with their partners is of paramount importance. As such, the standards developed by DHS must not only motivate organizations to dedicate resources to share but must also align them with evolving individual organization value assessments.

As it enacts the vision of the EO, DHS must put in place programs and funding to carry out the intent and not simply the spirit of the EO.

CHANGE THE ENGAGEMENT

Adopt flexible engagement approaches that help organizations improve protection of their communications and information infrastructures.

The value of threat intelligence sharing comes not from a few but in the many, typically the very entities that are under attack from cyber actors. These organizations are diverse with different infrastructures and solution needs. DHS must champion initial ISAO participation and help facilitate solutions *while recognizing* the ISAOs' need for flexibility to contribute their own tailored innovative approaches. This dual responsibility of DHS — to provide a flexible and supportive framework to bring organizations to the table, yet still allow them the autonomy to protect their own infrastructures — is essential for long-term benefits and enduring protection strategies.

Specifically, DHS must work with organizations on identifying the business risks that individual sectors face. Understanding stakeholders whose missions are most critical from a homeland security perspective will strengthen the development of appropriately tailored protection strategies while effectively sharing our resources.

The government should:

- Building upon the Section 9 List,[2] identify those organizations whose infrastructure is most at risk and whose protection is most critical to assuring national prosperity, security and public safety.
- Prioritize the development of closer ISAO partnerships with those organizations most at risk.
- Identify and work with influential organizations to increase national awareness of the issues facing ALL constituents.
- Understand the business of the Internet and focus its internal programs on identifying, monitoring and characterizing only those threats that have strategic significance to the nation's security and where the U.S. government can engage to help the private sector.
- Tailor engagements by understanding each ISAO partner's needs and operating environments and collaboratively developing and implementing approaches to address their specific risks.
- Provide options for ISAOs to effectively and uniquely define and promote value to their stakeholders.
- Increase opportunities for ISAO partners to expand their own knowledge and expertise.

FULLY AND PUBLICLY COMMIT TO A DUTY TO SHARE

Enable rapid, consistent sharing of valuable information as close to the point of information creation as possible.

As the EO directed, essential to addressing the threat environment is the ability to quickly share threat and mitigation information across organizations so that other organizations can rapidly understand, adapt to and address changing conditions. This requires shifting from an environment where a "duty to share" becomes the norm and "need to know" becomes the exception.

Convening safe, effective, non-attribution ISAO environments may require seed funding to help get them off the ground and to "prime the pump" with tools, techniques, processes,

[2] Executive Order 13636 - Improving Critical Infrastructure Cybersecurity February 12, 2013

templates, lessons learned and threat data. Bringing a greater consistency to information sharing will allow organizations to place greater focus on addressing and responding to or preventing threats, rather than getting the information in the first place.

The government should:

- Actively advocate and promote "duty to share" concepts and ideas in all it does.
- Working through its standards organization, understand and address the policy, procedural and technical barriers that inhibit sharing.
- Working in partnership with the Small Business Administration, NIST and other organizations, DHS should provide "starter kits" for ISAOs consisting of initial funding where appropriate and capabilities to remove as many of the barriers as possible to enable this commitment to sharing.
- Leveraging its current private sector partners, identify, fund and support the establishment of new ISAOs by promulgating the standards, tools and best practices to key lifeline sectors and critically focused regions.
- Fully commit to the ongoing sustainment of these ISAOs by helping them expand their value to both their individual members and the broader information sharing ecosystem through the following actions: engaging these ISAOs routinely in national exercises; convening threat exchange forums; and providing opportunities to the entities to represent the interests of the ISAO in a dialogue with the research community and in development of additional standards.
- Continuously seek opportunities to support mechanisms and standards that enhance sharing of relevant threat information and mitigation approaches across and between partners, regardless of the direct benefit to the government.

CHALLENGE THE MARKETPLACE

DHS must continue to challenge the marketplace to deliver effective products and services that reduce mission and business risk. Today's markets do not yet provide the full range of products and solutions required to securely and reliably address the threat environment. Moreover, market needs shift quickly as threats change. At the same time, consistent standards are an essential foundation for sharing information across organizations and developing interoperable technologies. DHS' engagement with the breadth of organizations that rely on communications and information infrastructure should enable them to identify and communicate emerging market needs. DHS should support a range of activities to enable development of a range of more innovative products and solutions that, in part, enable organizations to better and collaboratively address common threats.

The government should:

- Identify and communicate emerging technology needs and foster innovations to address those needs.
- Connect users to available and emerging solutions.
- Support standards adoption through appropriate research, development and testing.

STRENGTHEN AGILITY

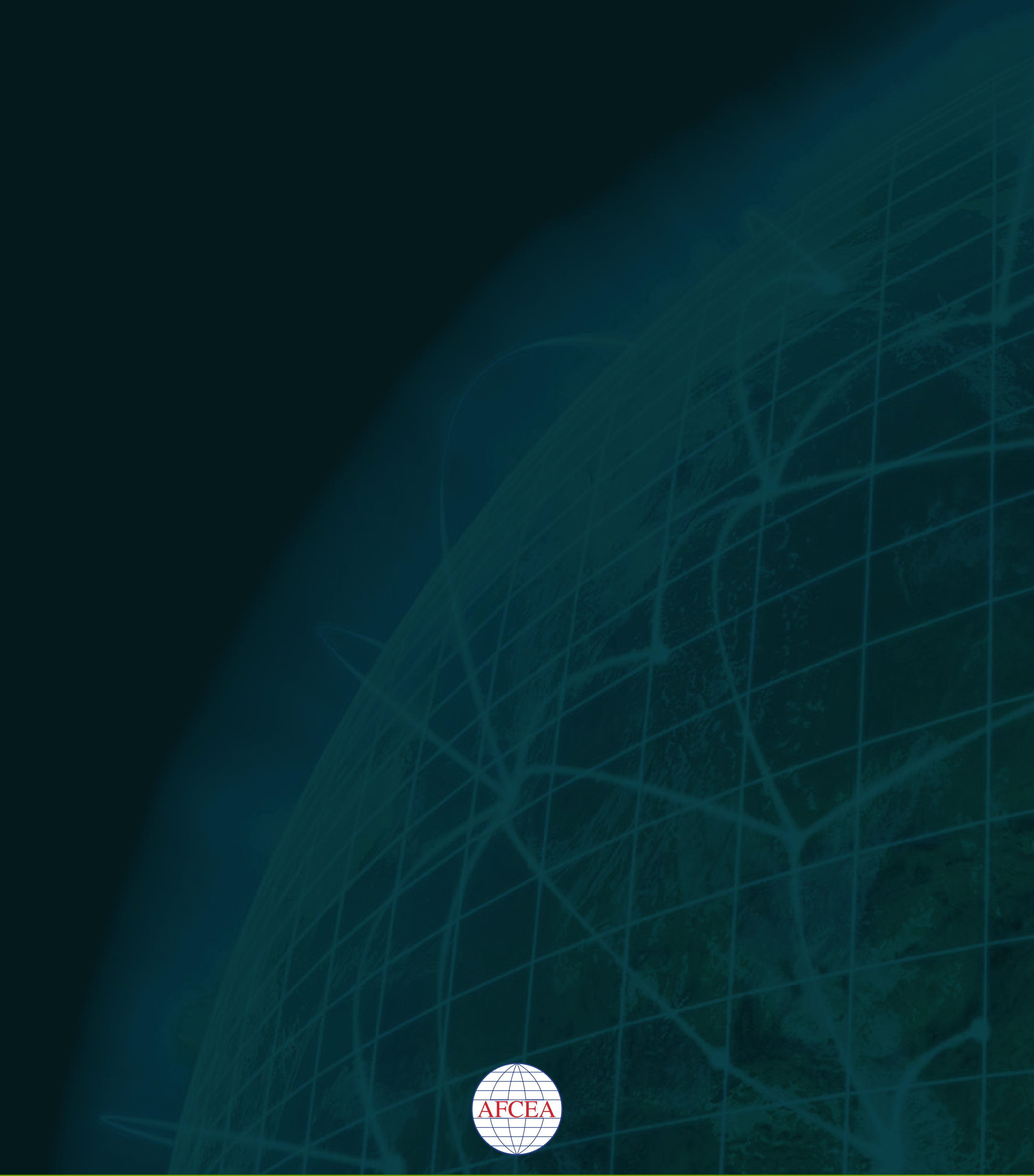
Enable operational agility to threats before, during and after incidents occur.
Effective operational response is required to address the potential harm caused by attacks or disasters affecting critical communications and information infrastructure. In this environment, distributed response models are the norm, making control inherently diffuse and requiring agility. DHS should strengthen analytic capabilities that enable partners to continually understand the environment so that anomalous threats can be better spotted, addressed, countered and constrained. The goal is to prevent attacks through effective analysis of shared information. Focus also is required to collaboratively define coordination models that enable effective action across a network of organizations. Strengthening these models will enable organizations to work in a more consistent way with their partners so they can jointly respond to changes in the environment more effectively.

The government should:

- Work with all ISAO partners to actively identify, coordinate and support responses to incidents that may cause significant harm.
- Identify and promote coordination models appropriate to the environment.
- Improve the sophistication, comprehensiveness and utility of analysis and mitigation approaches.
- Strengthen the skills of analysts and equip them with the necessary resources, processes and tools.

SUMMARY

The AFCEA Cyber Committee strongly supports the objective of improving our nation's ability to deter cyber attacks. Properly focused, the guidance in the recent executive order can be of great benefit toward achieving this objective. The observations and suggestions in this paper provide what we believe to be sound approaches for establishing a successful cyber information sharing infrastructure. The committee will continue to assess the area of information sharing and provide additional papers, as appropriate.



The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber