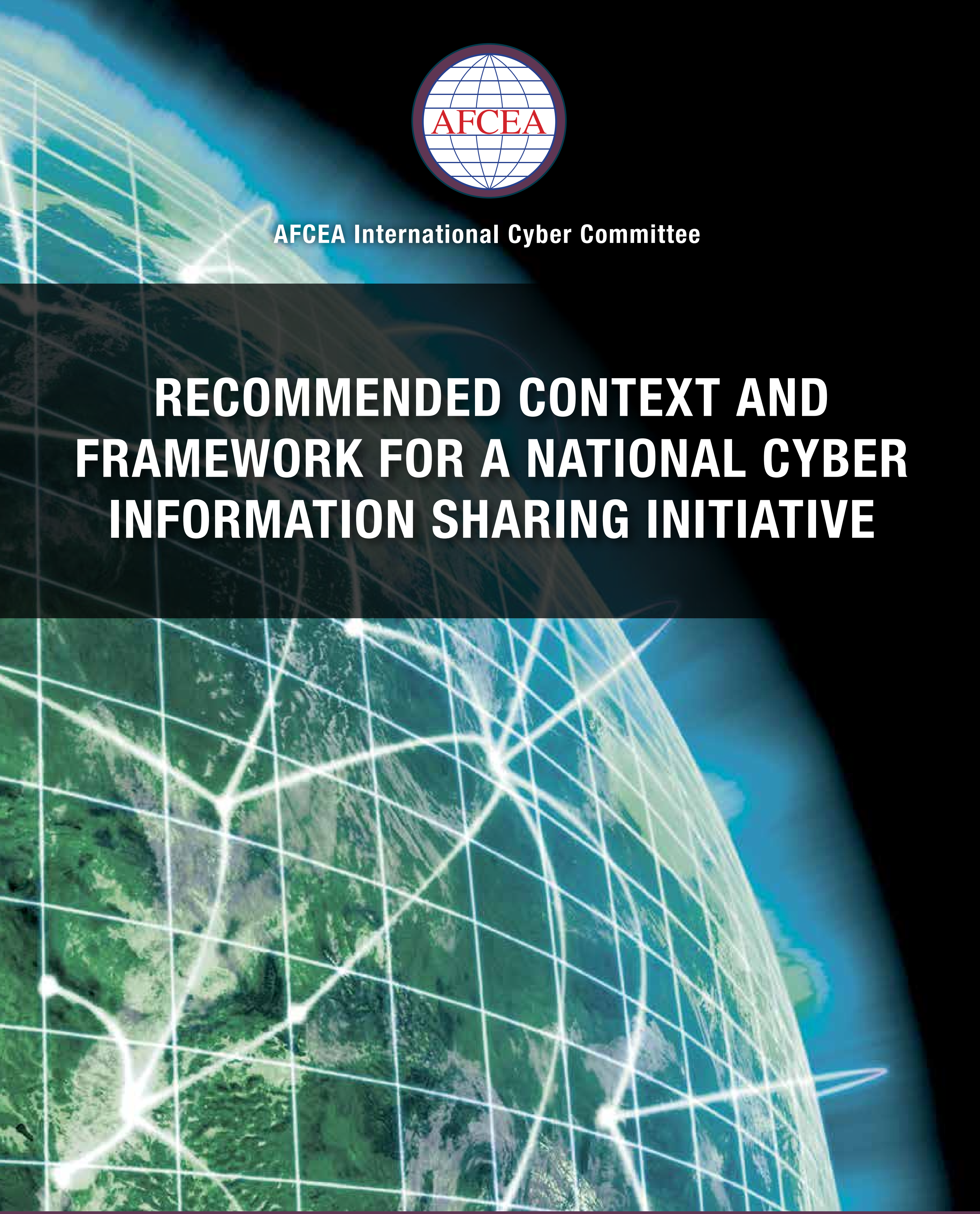


AFCEA International Cyber Committee

RECOMMENDED CONTEXT AND FRAMEWORK FOR A NATIONAL CYBER INFORMATION SHARING INITIATIVE

June 2016

INTRODUCTION

There has been increased public dialogue recently regarding the importance, potential benefits and urgency of sharing cyber-related information. The inference from much of the dialogue is that information sharing is viewed as a primary means to improve the nation's cybersecurity posture. AFCEA's Cyber Committee has been evaluating the topic of information sharing. In the fall of 2014, the committee assessed the nation's needs for information sharing and developed a set of recommendations that were provided to the White House team developing executive order[1], Promoting Private Sector Cybersecurity Information Sharing. The committee has subsequently reviewed the executive order and its recommended actions to implement a robust national information-sharing infrastructure. The committee observes that there are many solid and beneficial aspects of the executive order. However, it believes a successful implementation of the order requires an appropriate context for these efforts, as well as a framework that could be used to define success. This paper provides additional recommendations for establishing the standards and implementation of an effective **National Information Sharing Infrastructure.**

A CONTEXT FOR INFORMATION SHARING

The committee believes it is essential to recognize that the objective of information sharing must not just be the exchange of cyber-related information. Rather, information sharing must be recognized as a means to an end. The ultimate objective is enabling members of the cyber ecosystem to make defensive risk-based decisions based upon much more precise data. That is, the act of exchanging or sharing information is necessary but not sufficient to prevent cyber attacks.

Unfortunately, the term "information sharing" has become a misnomer. Enabling individual members of the ecosystem to achieve greater visibility into the threats they face by actively exchanging relevant data with other trusted members assists these organizations in taking advantage of the collective wisdom of the group. Achieving the desired objective requires not only the sharing or exchange of relevant information but also the employment of appropriate

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

analytical methods and tools that turn shared information into actionable products, either narrative guidance or automated means to block potential cyber attacks. **Therefore, the committee recommends that appropriate emphasis be placed on the analytical methods and tools as information sharing standards and implementation strategies are developed.**

INFORMATION SHARING FRAMEWORK

The committee also believes an appropriate model for implementing the information sharing requirements of the executive order is helpful to guide implementation efforts. In this regard, the operating methods of the National Weather Service (NWS) or the Centers for Disease Control and Prevention (CDC) are appropriate models. In both examples, there is an abundance of decentralized information exchanged with and among reporting organizations, but the primary value of the NWS and CDC is in the analytically derived products they develop. These products are then distributed in the form of weather warnings or health guidance to help save lives. These products are distributed to specific geographic regions or target populations as appropriate.

For our nation's cyber infrastructure, we need a National Information Sharing Infrastructure where the information exchanged is first appropriately analyzed so proper warnings or recommended actions can be disseminated to target audiences. Key to the success of this infrastructure is a tailored approach to the analytical products so they meet specific needs of a highly diverse set of audiences—such as government; large, mid size or small companies; specific industries; and private citizens—with each having unique cyber information sharing product needs.

To help guide the development of a National Information Sharing Infrastructure, the committee recommends that the effort be guided by a framework of principles and measures of success. This framework ensures the efforts are clearly grounded in the broader context for information sharing and the appropriate objectives.

Key principles of a National Information Sharing Infrastructure:

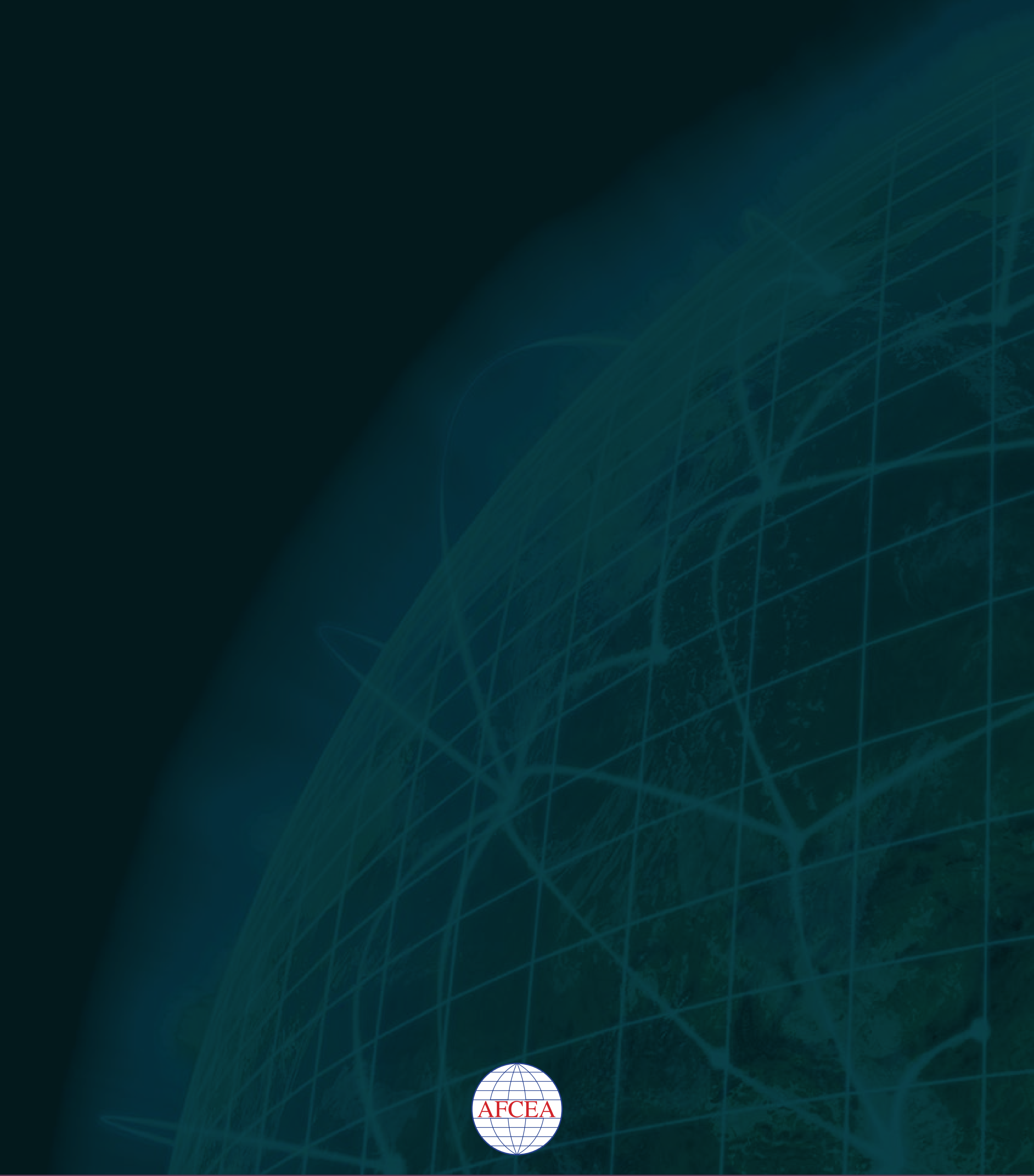
1. A mesh of multi-directional information flows;
2. Multiple nodes performing analysis of shared information leading to intelligence-derived recommendations and products;
3. Responsiveness to the different time sensitivities of multiple customers and audiences; and
4. A design that is resilient against attack and compromise with a strong focus on the integrity of the analytics being reported.

Recommended measures of success for a National Information Sharing Infrastructure:

1. Breach or attack is prevented or detected in time to allow a defender to make a risk-based decision on action;
2. Cybersecurity-related investments are realigned or increased;
3. Identification of attack patterns leads to changes in standard, commercial products that negate the attack;
4. Increased awareness and creation of a culture of cybersecurity at all levels, from organization executives to individual cyber systems users; and
5. Value derived from measures 1 to 4 to entice organizations to participate in sharing their information among all stakeholders, including private, public and academic organizations.

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 recommendations in this paper provide what is believed to be the necessary context and framework for building a successful National Information Sharing Infrastructure. The committee will continue to assess the area of information sharing and provide additional papers, as appropriate.



AFCEA

The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber