UNDERSTANDING CYBER SECURITY AND HOW IT AFFECTS FEDERAL GRANT WRITING

By Stephen R. Galati, CGW, AMP.APMP

With the prevalence of Internet accessibility and worldwide connectivity ingrained within all aspects of American life, cyber attacks have now become an imposing security threat to the Federal Government, U.S.-based businesses, and to all American citizens.

According to the University of Maryland – University College (2013), cyber security focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and digital spying are the top threats to national security, eclipsing terrorism. Sadly, cyber attacks are happening every day to the federal government and have become a serious "all government" issue.

Building cyber security as a core capability for the country has become a significant factor in federal grants and emergency planning. Establishing national cyber security capabilities will provide the foundation on which to build operational functions in cyber response and recovery, and enhanced coordination of activities though all levels of the federal government. As such, funds from each of the Homeland Security Grant Program (HSGP) components – State Homeland Security Program, Urban Areas Security Initiative, Metropolitan Medical Response System, and Citizen Corps Program – can be used to invest in functions that support and enhance State, Local, Tribal, and Territorial (SLTT) cyber security programs.

As a grantwriter, this means that cyber security elements will creep into your federal grant applications. A better understanding of cyber threats and security measures will ultimately help strengthen your grant applications and improve your ability to secure the funding. Some areas where cyber security will surface include equipment investments, planning, training, drills and exercises, and personnel. To gain a greater understanding of cyber security related to the federal government, you need to understand the state of cyber security legislation, recognize cyber information resources, and learn how to stay in the know.

The Long Road to Passing the Cybersecurity Act of 2012

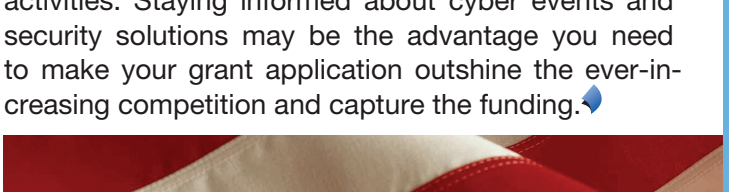
The Cybersecurity Act of 2012, introduced by Senators Joseph Lieberman [I-CT] and Susan Collins [R-ME] to the Senate in February 2012, called for the establishment of a National Cybersecurity Council to focus on cyber risk assessments, identification of critical infrastructure, cybersecurity practices and procedures, and technical guidance. The bill was passed by the House of Representative previously, but stalled in the Senate. It was reintroduced in July 2012, but did not receive the required votes to pass. In February 2013 as an effort to fill the gap in legislation, President Obama released an *Executive Order on Cybersecurity* and the *Presidential Policy Directive on Critical Infrastructure Security and Resilience* (see the Resources section below for more information). With the Executive Order and Presidential Directive in place, the government can remain focused on cyber attacks and security practices, share cyber security-related information, and continue to rewrite the Cybersecurity Act of 2012 so that it can be passed into legislation (ASIS, 2013).

Write Provocative Grants by Staying Informed about Cyber Events

The United States Government is now hyper-aware of the dangers of cyber attacks and is taking a leadership stance on cyber security and information dissemination. As such, the Department of Homeland Security organized the United States Computer Emergency Readiness Team (US-CERT) to lead the government's

efforts to "improve the nation's cyber security posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans" (US-Cert, 2013, ¶ 1). Understanding what the US-CERT does, the information they provide to citizens, and the affiliations they have with major corporations such as Microsoft, Apple, and over 250 other organizations, will arm grant writers with the necessary information needed to incorporate sensible, effective, compliant, and provocative solutions within their grant applications.

So, as a grant writer, how can you stay informed about cyber events and cyber security information? One easy and effective way to stay informed is through the National Cyber Awareness System (NCAS), a dynamic information alert system that makes available up-to-date cyber security information. NCAS provides information on current security-related activity, avails alerts to your email address, provides weekly bulletins of new vulnerabilities, and provides tips on common security issues facing the general public. All of this information is useful when writing federally-funded grants where there is money tied to cyber security activities. Staying informed about cyber events and security solutions may be the advantage you need to make your grant application outshine the ever-increasing competition and capture the funding.



Blueprint for a Secure Cyber Future

The Cybersecurity Strategy for the Homeland Security Enterprise

November 2011

The Department of Homeland Security's Blueprint for a Secure Cyber Future represents one framework within which stakeholders in government, the private sector, and international partners work together to develop cybersecurity capabilities.

Although they may not fully grasp the technical requirements of cybersecurity, funders generally support the cost of securing the technology that will be purchased with grant funds, if the applicants request funding for that purpose.
(Department of Homeland Security Document)

CYBER SECURITY RESOURCES

Whether you are new to cyber security or have been involved with cyber security issues in the past, the following resources will be useful tools to your grant writing arsenal.

1. Fact Sheet: Executive Order on Cyber Security / Presidential Policy Directive on Critical Infrastructure Security and Resilience

http://www.dhs.gov/news/2013/02/13/fact-sheet-executive-order-cybersecurity-presidential-policy-directive-critical

2. Cyber Security Legislation and Revised Cyber Security Act

http://www.hsgac.senate.gov/issues/cybersecurity

3. Cyber Security Overview

http://www.dhs.gov/cybersecurity-overview

4. The National Strategy to secure Cyberspace

http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

5. The Comprehensive National Cyber Security Initiative

http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

6. DHS Cyber Security Publications

http://www.dhs.gov/cybersecurity-publications

7. Ancillary Cyber Security Information

http://www.dhs.gov/topic/cybersecurity

8. US-CERT National Cyber Awareness System

http://www.us-cert.gov/ncas

9. FY2013 Homeland Security Grant Program Supplemental resource: Cyber Security Guidance

http://www.fema.gov/library/viewRecord.do?id=7495

References

ASIS. (2013). Cybersecurity. Retrieved from https://www.asisonline.org/Membership/Government-Affairs/Legislative-Center/Pages/Cybersecurity.aspx

University of Maryland – University College. (2013). Cyber security primer. Retrieved from http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm

US-CERT. (2013). About us. Retrieved from http://www.us-cert.gov/about-us