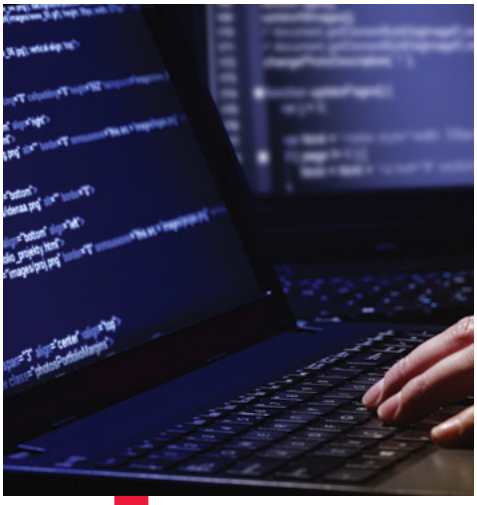
AN ALERT FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

BDO KNOWS:
GOVERNMENT CONTRACTING



CYBERSECURITY ALERT
Protecting Cyber Networks Act: Impact on Government Contract and Grant Recipients

Government contractors have been faced with a number of new standards and regulations in regard to cybersecurity – with only more to come in the upcoming year. Contractors are faced with challenges on how to understand, implement and prepare for these regulations. What will be critical for organizations in the coming months is to build awareness around the obligations and to conduct a thorough review of their existing cyber policies and programs to ensure compliance with the new mandates. This alert focuses on the recent Protecting Cyber Networks (PCN) act passed by the U.S. House of Representatives and previews the potential impact this will have on reporting for contractors in 2015.

BACKGROUND

In the wake of recent high profile cyber attacks on American businesses and government agencies, lawmakers in the House passed the Protecting Cyber Networks Act (PCNA) on April 22, 2015. The bill was designed to confront the growing number of cyber threats facing the country by facilitating increased sharing of cyber threat indicators and defensive measures both among contractors and between contractors and the federal government. [1]

PURPOSE

According to the bill's proponents, voluntary information sharing within the industry will help businesses defend themselves more effectively against cyber attacks. In addition, information sharing with the federal government will enable more efficient communication regarding cybersecurity concerns between the public and private sectors and allow both to detect and mitigate vulnerabilities more quickly. Critics of the bill argue that it will infringe on personal privacy rights and primarily serve as another mechanism to transfer personal information to surveillance agencies.

THE IMPACT

The PCNA encourages businesses to voluntarily share cyber threat indicators with one another and with federal agencies—with the exception of the Department of Defense (DoD) and the National Security Agency (NSA). To alleviate concerns associated with the disclosure of personal

1 See PCNA Section 11 (5) definition of Cyber Threat Indicator and (6) for definition of Defensive Measure

For more information on the PCNA or ways in which BDO leverages its deep industry knowledge to strengthen your cybersecurity infrastructure, please contact:

ROBERT CRAIG
Managing Director
rcraig@bdo.com

NISHA GUPTA
Senior Manager
ngupta@bdo.com

MICHAEL PRUTSOK
Associate
mprutsok@bdo.com

▶Read more

information, businesses must scrub all such information from that which they intend to share. In exchange for this effort, and as long as it is done in good faith, businesses are granted some liability protection from legal action associated with accidental disclosure of information.

On Your Business:

While most provisions of the bill are voluntary, they may have an impact on your business. In particular, the bill:

- Permits voluntary sharing of a strictly limited category of information related to cyber threats and the defensive measures designed to combat them;
- Requires businesses to remove personal information prior to sharing cyber threat information with the industry or federal agencies;
- Prohibits the government from forcing businesses to provide information related to cybersecurity; and
- Provides a degree of liability protection for businesses that share information in good faith.

On Your Privacy:

The bill will also protect your privacy by:

- Requiring the federal agency that receives cyber threat indicators to perform a second scrub to remove personal information before sharing the indicators with other relevant federal agencies;
- Imposing strict restrictions on the use, retention and searching of any data shared by government contractors with the government voluntarily; and
- Enforcing strong privacy and civil liberties protections by permitting individuals to sue the federal government for intentional privacy violations in federal court.

Critics of the PCNA argue that its effectiveness will be limited by its inability to provide tangible, direct benefits to businesses choosing to share information with the government, thus reducing any incentive for industry's participation. Proponents believe this shortcoming will be overcome as government contractors see the direct benefit of information shared and develop an "in-kind" attitude toward disclosure under the PCNA.

BDO Knows Cybersecurity:

Our team of experienced professionals has extensive knowledge in the government contracts and grants industry and understands the critical importance of developing and implementing all aspects of secure information systems. We offer services to our clients with a full suite of compliance solutions to help you navigate the ever-changing landscape of the cyber world.