

MISSILE DEFENSE AGENCY

# Office of Small Business Programs

- CYBER SECURITY UPDATES -



## Message from the Director

Lee Rosenberg

As you are probably aware, cybersecurity is a big deal these days. Just look at the news and you will find all kinds of horror stories regarding sensitive information obtained through hacking of both Government and Civilian information systems. If you have been a victim, as have I and millions of other Government employees, you know that sinking feeling that you get knowing that your personally identifiable information is floating around out in cyber space, possibly in the hands of some who would do us harm by using that data. Now, look at a much bigger picture and think about the defense of our nation and the manner in which we go about provisioning ourselves for that defense. There is no doubt that all who are involved in that process are heavily dependent on the use of computers and electronic data to accomplish their work. As we transition to that cyber space to conduct business and to pass information, we bring with us unique security issues, which didn't exist 20 years ago. The Department of Defense (DoD) is beginning to realize the extent of our vulnerabilities in this cyber world, and is taking steps to protect our information from bad actors around the world, who would steal that data to increase their military capabilities while doing harm to ours. A lot of the data that needs protecting is not necessarily classified data. For classified data, we already have fairly robust systems to protect its unauthorized disclosure. The Department is now realizing that there is a plethora of data that is not classified, but that can provide potential adversaries with a wealth of information about our operations and systems. That brings me to the theme of this newsletter, and the information that you need to be aware of moving forward as a Defense contractor.

In August 2015, the DoD issued an interim ruling revising DFAR 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting and introduced two new mandatory clauses: 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls; and 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. MDA has begun implementing these on all new solicitations. These clauses will have significant impact on you as an MDA contractor or subcontractor. DFARS 252.204-7009 and DFARS 252.204-7012 are required to flow down by the prime through all tiers of subcontracting. That means if you are a lower tier subcontractor, you are just as affected by the clauses as the prime contractor.

So, what do these clauses do? DFARS 252-204-7012 requires Contractors (and Subcontractors due to the flow down requirements) to protect any DoD information provided to

the contractor or collected, developed, received, transmitted, used, or stored by or on behalf of the Contractor in support of performance of a Government contract. It now includes commercial goods as well. Protected information falls into one of the following categories:

(a) *Controlled technical information.*

(b) *Critical information* (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(c) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(d) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information).

These clauses also contain cyber incident reporting requirements, with which you must comply, and which may include reporting on compromises of proprietary data.

DFARS 252.204-7008 requires Contractors to comply with the security controls outlined in National Institute of Standards and Technology (NIST) Special Publication 800-171. You should be aware that there are new requirements in this publication that may cause additional capital investment in your information technology systems, and new training requirements to comply with the new requirements. There is a provision in the clause for you to put forward alternate methods for complying, but those must be approved by the DoD Chief Information Officer (CIO).

DFARS 252.204-7009 requires the protection of the cyber incident information that is disclosed and speaks to the obligations for non-disclosure of the information by third-parties, along with the possible civil and criminal penalties associated with the unauthorized disclosure.

All in all, these new cybersecurity requirements may have a significant impact on you both financially, and in your business operations. You should become very familiar with all requirements. Now is the time to assess your operations and

*Continued on Page 3*



# New Cybersecurity Regulations

Genna Wooten

The Department of Defense (DoD) decided to implement new cybersecurity regulations back in August of 2015, following the Office of Personnel Management's (OPM) breach of Data that impacted the Personal Identifiable Information (PII) of over 21 million government employees and contractors. The DoD stated that it decided to implement these rules because of the urgent need to guard information, understand the scope of cyber-attacks against contractors, and reduce the vulnerability of cloud computing attacks.

The new regulations require, among other things, that prime contractors and their subs employ "Adequate Security" and implement the security controls based on the National Institute of Standards Special Publication, titled "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". Contractors are obligated to report, within 72 hours of discovery, any cyber incident that affects the covered contractor's information system. The DoD understands that this can be a significant cost to Small Businesses, so we have published a list of resources on our website at [www.mda.mil](http://www.mda.mil).

Outside of the new DoD Cybersecurity requirements, here are 9 Cyber Security Tips for Small Businesses to help keep your data safe from cyber criminals:

## 1. Use the FCC's Small Biz Cyber Planner to create a cybersecurity plan.

The Small Business Cyber Planner, by the FCC (<https://www.fcc.gov/general/cybersecurity-small-business>), is valuable for businesses that lack the resources to hire a dedicated staff member to protect themselves from cyber threats. The tool walks users through a series of questions, to determine which cybersecurity strategies should be included in the planning guide, and generates a customized PDF that serves as a cybersecurity strategy template.

## 2. Establish cybersecurity rules for your employees.

Establish rules of behavior describing how to handle and protect personally identifiable information, and clearly details the penalties for violating cybersecurity policies.

## 3. Protect against viruses, spyware, and other malicious code.

Install, use, and regularly update antivirus and antispymware software on every computer used in your business. Such software is readily available online from a variety of vendors.

## 4. Educate employees about safe social media practices.

Depending on what your business does, employees might be introducing competitors to sensitive details about your firm's internal business. Employees should be taught how to post online in a way that does not reveal any trade secrets to the public or competing businesses. This type of safe social networking can help avoid serious risks to your business.

## 5. Manage and assess risk.

Ask yourself, "What do we have to protect? And, what would impact our business the most?" Cyber-criminals often use lesser-protected, small businesses as a bridge to attack larger firms with which they have a relationship. This can make unprepared small firms a less attractive business partner in the future, blocking potentially lucrative business deals.

## 6. Download and install software updates when they are available.

All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install such updates automatically.

## 7. Make backup copies of important business data and information.

Regularly backup the data on every computer used in your business. Critical data includes word processing documents, spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files; also, backup data automatically, if possible, or at least weekly.

## 8. Control physical access to computers and network components.

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft, so make sure they are stored and locked up when unattended.

## 9. Secure Wi-Fi networks.

If you have a Wi-Fi network for your home business, make sure it is secure and hidden. To hide your Wi-Fi network, configure your wireless access point, or router, so that it does not broadcast the network name, known as the Service Set Identifier (SSID). In addition, make sure that passwords are required for access. It is also critical to change the administrative password that was on the device when it was first purchased.



Continued from Page 1...

information technology infrastructure, to insure they comply with the new requirements. Now is also the time to implement the changes necessary to bring your business into compliance, if you plan to stay in the DoD marketplace.

As I mentioned earlier, cybersecurity is a big deal with the DoD. We are seeing that importance across all DoD operations, now including the procurement of goods and services to support our warfighters. In this edition of our newsletter, you will find helpful advice and information to assist you in your efforts. I urge you not to wait until the last minute to get your businesses into compliance, but assess your situation, now. Take those measures necessary to protect our valuable defense information from falling into the wrong hands.

## Safeguarding MDA Information

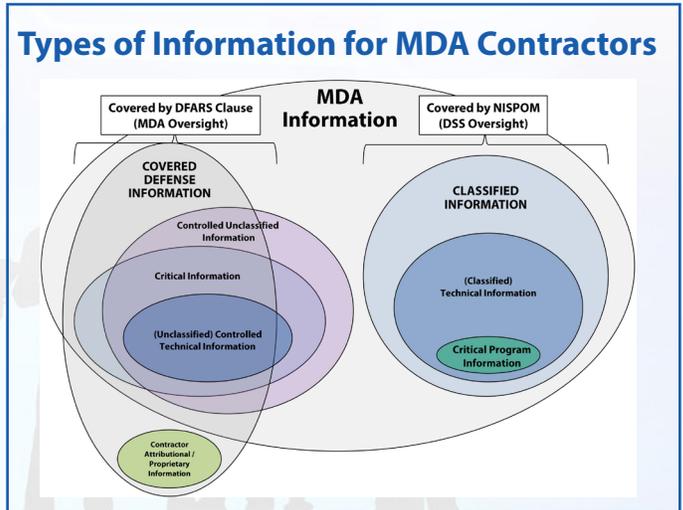
Jerrol Sullivan

Small businesses currently performing on MDA contracts as prime or subcontractors, and those seeking to do business with MDA in the future, must be aware of the implications of the August 26th, 2015 DoD interim ruling which revised DFARS 252.204.7012 to establish guidance for safeguarding unclassified DoD information. This interim rule is effective immediately, and is becoming increasing more prevalent in Missile Defense Agency (MDA) solicitations. This article intends to clarify the changes to this clause, and highlight MDA's oversight of the types of information handled by MDA contractors and requires protection. The following are highlights of the DFARS 252.204.7012 clause and the update:

- **DFARS Clause 252.204-7012, "Safeguarding Unclassified Controlled Technical Information", Published November 18, 2013**
  - Affects all contracts that contain, or will contain unclassified controlled technical information (UCTI)
  - Does not cover all Controlled Unclassified Information (CUI)... e.g., FOUO
- **DFARS Clause 252.204-7012: "Safeguarding Covered Defense Information and Cyber Incident Reporting", 26 Aug 2015 (updated)**
  - Covers all defense information to include Controlled Unclassified Information (CUI)...e.g., FOUO
  - Focuses more on technical controls (for industry as) established in National Institute of Standards and Technology (NIST) standard publication NIST SP 800-171
  - Flows to all subcontractors and suppliers, regardless of size, and to all tiers of the supply chain

- Requires that all Cyber incidents be reported via the DoD Defense Industrial Base (DIB) Cybersecurity Program portal (<http://dibnet.dod.mil>) within 72 hours of detection
- Requires that contractors support DoD damage assessments
- Requires contractors to identify deviations from NIST implementation guidance during contract proposals (DFARS provision 252.204-7008)

In summary, protection of MDA information is critical to preserving the intellectual property and competitive capabilities of the MDA industrial base, and the technological superiority of fielded Ballistic Missile Defense Systems (BMDS). MDA contractors and subcontractors, regardless of size or tier, within the BMDS supply chain, must provide adequate safeguards for MDA information by actively managing the Cybersecurity posture of their people, systems, and networks. Prime Contractors are responsible to report Cybersecurity incidents involving MDA information, both directly to MDA and via Defense Industrial Base Network (DIBNet), then work with MDA to assess any damage.



\* Handled as CUI within DoD Defense Security Service (DSS) National Industrial Security Program Operating Manual (NISPOM) (DoD. 5220.22-M)

## Outreach Efforts to Provide Small Business Community with Cybersecurity

Laura Anderson

**ALL** defense contractors and subcontractors, including small businesses, must protect their networks and data, as required by certain clauses within the Department of Defense (DoD) contracts. As outlined in the U.S. Government Accountability Office's report (GAO-15-777) on Defense Security, "Small businesses, including those that conduct business with DoD, are vulnerable to cyber threats and may have fewer resources, such as robust cybersecurity systems, than larger businesses to counter cyber threats". Knowledge is empowering. To better position defense small businesses in protecting information and networks from cyber threats, the Missile Defense Agency (MDA) Office of Small Business Programs (OSBP) has compiled a listing of Cybersecurity Resources.

For a complete listing of the Cybersecurity Resources compiled by the MDA OSBP, please go to [http://www.mda.mil/business/smallbus\\_programs.html](http://www.mda.mil/business/smallbus_programs.html)

## How do the New DoD Cybersecurity Requirements Affect MDA's Future Market Research

Becky Martin

The Department of Defense (DoD) has initiated new mandatory cybersecurity requirements for all DoD procurements. These new cybersecurity requirements will affect all areas of contracting within the DoD. Here we are going to discuss how it will affect future market research. In concert with other data that MDA reviews during market research, cybersecurity requirements will now be a critical part of determining a small businesses' ability to perform all of MDA's requirements. MDA will need to be confident that SBs will be able to comply with the cybersecurity requirements, as well as other technical capabilities. It will also be critical that SBs are able to communicate these new cybersecurity requirements with their subcontractors. For additional information on the new cybersecurity requirements, please visit [www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses](http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses).

## Cybersecurity and Mentor-Protégé Program

Ruth Dailey

The Mentor-Protégé program is also working to comply with the Implementation of DFARS Rule 2013-D018. For any new Mentor-Protégé agreement, we have added a new task that all mentors need to implement. "Security - Computing, Facility and Cyber: Protégé requires the security of its employees and its assets (tangible and intangible) to be of primary importance of its continued growth, profitability and success. The continued strengthening of security controls and procedures is essential for the protection of employees, the preservation of assets, and the effective enforcement of rules and regulations.

Protégé wishes to enhance its proactive security program, by establishing a robust and secure computing capability, to minimize security risks and business losses, and to comply with all regulatory requirements. This will present additional growth opportunities for growing small businesses. Mentor will provide training and guidance to help Protégé develop and address growing vulnerabilities to computer systems. This will support future contracting efforts with Department of Defense (DoD) and prime customers for classified and unclassified operations and requirements."



As we move forward, we need to be diligent on cybersecurity requirements of DoD information on contractor systems and help the DoD to mitigate the risks related to compromised information, as well as, gather information for future improvements in cybersecurity policy by training small businesses on the importance of safeguarding DoD information.