



Summer 2016

# Information Security 101

## Inside this issue:

Government and Business Partner in New Cybersecurity Plan

Compliance Corner: What is FISMA?

Uncle Sam wants YOU...to take more training!

Pokemon? No

ARC Program Update: Greenland Deployment Success

ARC IT Spotlight: Craig Bussard, Information Security Team

## Government and Businesses Partner in New Cybersecurity Plan

In late July, President Obama issued a Presidential Policy Directive providing new guidance to government agencies and private companies on how to partner in the face of a cybersecurity incident. The primary objective of the new policy directive is to outline channels through which private entities can report cyber incidents to the government for tracking purposes and to request support in resolution of those attacks. The policy is based on a principle of shared responsibility between individuals, government, and the private sector to protect cyberspace as a matter of national security and general wellbeing. Improved information sharing about attack types, vectors, and frequency will allow government agencies to mount an appropriate response based on a well-informed understanding of the real risk of security incidents. The policy emphasizes cooperation, and is careful to enumerate the importance of confidentiality when it comes to the details of any particular security incident. Companies worry that public knowledge of a hack will impact the bottom line, so discretion on the part of the government will

be paramount if the public/private partnership is to be effective. While there's a great deal of responsibility placed on private companies by the new directive; it is hardly a one way street. Key provisions are in place to provide restoration support for an organization that falls victim to a security incident. Commitment of the appropriate law enforcement agencies is also addressed. Some reporting was already happening on a national scale, but the president's recent directive provides clear contact information for how and when companies should report cyber incidents and establishes a task force to oversee the federal response., unifying activities that had previously been stretched across numerous government agencies.

Learn more about the details set forth in the plan by reading the complete policy directive. The full text is available online from the White House press office at:

<https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

## Compliance Corner: What is FISMA?

Features within the Information Security Newsletter often address topics under the umbrella of "FISMA Compliance." But if your regular job role doesn't involve an IT security function, you may not be familiar with FISMA or what it means to the Arctic Program. The acronym FISMA originally referred to the Federal Information Security Management Act of 2002, the stated purpose of which was to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information re-

sources that support Federal operations and assets." FISMA established a framework, a set of standards to which all federal agencies would be held to ensure each was doing its due diligence in protecting the data entrusted to it by the American people. Many federal compliance requirements related to the use of IT resources, phones, and the internet have their roots in FISMA. Most agencies undergo regular compliance audits against the standards as they are updated. Today, FISMA may also refer to the Federal

Information Security Modernization Act of 2014. FISMA 2014 places responsibility for the management of information security policies within the Department of Homeland Security (DHS), and codifies DHS's role in creating information security policies and overseeing federal agencies' compliance with those policies. Even without regular audits, FISMA establishes an industry best-practice for information security, and its guidelines establish a strong foundation for any agency information security program.

## Uncle Sam wants YOU....to take more training!

A lot stands to change in this year's presidential election, but one thing is for sure: our nation's next president will have the responsibility of setting the agenda for national security, and that includes defending the country's latest final frontier - cybersecurity.

But the president can't do it alone! Cybersecurity is everyone's responsibility, and protecting our data in cyberspace begins with you. As a participant in a federal program, individuals affiliated with the Arctic Program have an increased responsibility to be prudent when it comes to protecting information assets.

Taking adequate training is a great start to doing your part. Annual training provides a refresher on common attack vectors and may help you prevent a costly cyberattack on your organization. Each quarter, we feature news articles, security tips, and useful information related to information security in this newsletter. Reading the newsletter regularly is a great way to stay informed of the latest trends and do your part when it comes to protecting program data.

The Information Security team wants to ensure you have access to the right training to be successful when you face common information security challenges in the workplace. That's why we encourage all readers to take the free online Cybersecurity Awareness Challenge offered by the Defense Information Systems Agency (DISA), which is available online at <http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm>

In addition to this issue of the newsletter, a direct link to the training will also be added to the Arctic Program RSL Resources page where you can also find archived issues of the Information Security Newsletter and other helpful resource documents [http://www.nsf.gov/geo/plr/arctic/res\\_log\\_sup.jsp#itsec](http://www.nsf.gov/geo/plr/arctic/res_log_sup.jsp#itsec).



## Pokemon?...No

It's ok to admit it...have you been outside chasing Pokemon? The unique mobile game swept the country by storm this summer, but did you know that the app brought with it a wealth of new security concerns? When it was first released, an error in the application programming allowed the app full permission to a user's private emails account and photos, including the ability to send, edit, and delete. That vulnerability was fixed in a matter of weeks after the release, however the inherent functions of the game require users to relinquish a significant amount of data from their phones including GPS location, access to the camera, and more. Mobile applications in general tend to be more risky than web-based programs because mobile technology is newer and still developing. That means hackers and companies who develop devices and apps are working at the same time to develop (and for hackers, break) the best code. Apps also require a lot of information from phones to operate properly, which may be different from information collected on the web. And

what happens to all that data you may wonder? That's another problem with apps, downloading them often requires the user to agree to share data with third-parties who may use or sell information without further explicit consent.

So what's a fun-loving adventurer to do? Well, only you can decide if the privacy risks associated with any mobile app are a good choice for you, but it is important to remember how use of your mobile devices may interact with your responsibilities as a member of the Arctic team. Think critically about the information you may inadvertently put online by taking pictures in your workplace. Could online pictures of your office might put your information or facility at risk? Individuals with IT roles must pay careful attention to the sites they access and should set a good example for their team by reviewing the security and

privacy details of any app or device before participating in its use. And of course, use of games or personal apps, especially those that release large amounts of private data, is never appropriate on a government mobile device. Review your organization's mobile device policy for more information. And in the meantime, go ahead and take that walk outside, just leave the Pokemon behind.



# ARC Program Update: Greenland Deployment Success

Arctic Sciences Section  
Information Security  
Support is provided by  
SPAWAR Office of Polar  
Programs (SOPP)

Robert Myer, Program  
Manager, SOPP  
843.609.7753  
robert.l.myer.civ@mail.mil

Maria Petrie  
Arctic Information Security  
706.414.1412  
petrie\_maria@bah.com

Craig Bussard  
Arctic Information Security  
843-277-6264  
cabussard@techsoft.com



This summer, the Information Security Team focused on preparing for a successful deployment to the Arctic sites in Greenland. As a reminder, site visits are an important way for the Information Security team to get a hands-on understanding of the day-to-day activities and the sites. The more we know about how information is used in the program, the better we can work to keep it safe and secure! Security Control Assessments were successfully completed at Summit and Kangerlussuaq Stations, and IT Contingency Planning Lifecycle activities continue for the Summit Station now that the team is home. The team was thrilled with the advances in information security that the onsite staff demonstrated during the visit. Awareness and due diligence on the part of every staff member can

go a long way when it comes to keeping data in the Arctic program safe. As a result of the deployment, the team will create a report for the program managers that outlines how the program has grown over the time since

the last on-site assessment, and what potential risks will require attention over the next year to resolve. Thank you to everyone who made this year's deployment to Greenland a great success!



## ARC IT Spotlight: Craig Bussard, ARC Information Security Team

Membership on the Arctic Information Security Team is not for the faint of heart! In addition to technical acumen, it requires travel to remote areas and a willingness to venture out in extreme weather—not things you find in every IT job! This month's IT Spotlight is the latest brave member to join the team—Information Assurance Analyst Craig Bussard.

Q: What's your background? How did you come to support the Arctic program?

A: I've spent 6 years providing Information Security support to various Department of Defense programs, from United States Marine Corps to Joint Task Force Medical to US Army Corp of Engineers. I've always had a passion for scientific research, so when I had a former manager reach out to me for the position – I jumped on it.

Q: What do you most look forward to doing as part of the Arctic team?

A: I have been most excited about the experience to travel to the Arctic Circle. Going to Greenland was an incredible time. I really took an appreciation for how science-focused the programs were. Getting to visit Kangerlussuaq and Summit Station are two things I never imagined would be doing.



Living in Charleston, South Carolina – the climate was unlike anything I had ever seen. The miles and miles of snow at Summit Station, the edges of the glacier, all incredible!

Q; What's the most interesting thing you've learned on the team so far ?

A: The most interesting thing I've learned so far is probably the "Clean Air" area at Summit Station. Due to the altitude and remote location – some scientific experiments are able to run up there in some of the cleanest air on Earth! All of the climate research was fascinating.

Q: From a personal standpoint, what are you excited about right now?

A: Well, big news for my family. Me and my wife are expecting our firstborn in late August! It's an exciting, and slightly terrifying, time!