Information Security and the Outsider:  
Part 2 – CAP as a Case Study

by M. E. Kabay, PhD, CISSP-ISSMP  
Associate Professor of Information Assurance  
School of Business & Management  
Norwich University, Northfield VT

In this two-part series, guest writer Lt Col LTC Robert E. Jennings<http://www.linkedin.com/in/simplecaveman>, Vice Commander of the New Jersey Wing of the Civil Air Patrol<http://encampment.njwg.cap.gov/welcome08.htm> – and a leader of the Service Delivery Managers in Dell Computer’s ProSupport organization<http://www.dell.com/prosupport> – looks at how the US Government is working with semi-official volunteer organizations. In this part, he looks more closely at how Civil Air Patrol, the all-volunteer, civilian auxiliary of the US Air Force, introduced more rigorous information security practices to better serve new domestic missions from the Government.

The remainder of this column is entirely Lt Col Jennings’ work with minor edits.

* * *

The orientation of Civil Air Patrol (CAP)<http://www.gocivilairpatrol.com/>, as an example, used to be easy and straightforward. As the congressionally chartered auxiliary of the U.S. Air Force, CAP performed most of the inland search & rescue in the United States on behalf of the Air Force and provided aviation, communications and people assets in relief of disasters. In the 1990s, CAP began using its light aircraft fleet to provide reconnaissance of domestic drug growth for federal, state and local law enforcement agencies.

9/11 was a transformational event for every government organization and person concerned with information security. CAP aircraft were the first non-military planes in the air after the attacks, using high-resolution digital cameras and satellite uplinks to transmit images of Ground Zero and other areas of interest to National Command Authorities. Since 9/11, CAP’s missions have grown to include more and more homeland security elements, focused around their unique aviation capabilities.

Traditional information security in the United States’ government is based on a series of United States Code and Executive Orders that have evolved since World War II. Information can be classified as Confidential, Secret or Top Secret, with a number of modifiers such as compartmentalization or nuclear weapons design. While not an official part of the current classification structure, there are administrative designations for unclassified information, such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU).

The level of access that a person can have to classified information in the US is based on the level of investigation they are put through. Anyone who enters the military receives a National Agency Check (NAC)<http://www.tpub.com/content/aviation/14243/css/14243_219.htm> and is usually cleared to handle information classified as Confidential. A NAC investigation also generally permits interim access to Secret information, while a more thorough Background Investigation (BI) is performed, which generally takes 4 to 6 months. A successful BI allows access to Secret information and certain Top Secret material. For more highly sensitive material, such as nuclear weapons, encryption and high resolution satellite imagery, a more extensive
Special Background Information (SBI) is conducted, which can take up to a year. The US Government is exempt from the Employee Polygraph Protection Act (29 USC 2002 <http://www.law.cornell.edu/uscode/html/uscode29/usc_sec_29_00002002----000-.html>, and certain high level positions in the Defense and Intelligence communities require successful completion of a polygraph test.

As for all classified information, a certain level of clearance does not automatically offer a person access to all information classified at that level. A need to know is required in combination with the appropriate level of clearance.

The volunteers of Civil Air Patrol are civilians from all walks of life. Although many of them have military or government services backgrounds, the majority do not. There is also a cadet program for youth from 12 to 18, and some of the older teenagers participate in the operational missions. One small advantage CAP offered as the government needed to reach deeper for homeland security resources was that its adult members had been required to submit a fingerprint card and undergo an FBI NAC since the early 1990s. The original purpose of this was to protect the teenagers in the cadet program (CAP was the first national youth organization to fingerprint and check the backgrounds of its adult members), but it has proven useful to provide some level of vetting for their members to be trusted with information related to military and homeland security missions.

Building on this existing corps of volunteers that were 100% background checked, CAP began building a catalogue of its members that had existing government security clearances. Members went to a secure online Web application to self input their security clearances, which were then verified through the Air Force’s CAP liaison unit. In conjunction with this effort, Civil Air Patrol introduced mandatory Operational Security (OPSEC) training modeled on the military’s OPSEC training for new recruits. OPSEC training is designed to make a person aware of the sensitivity of information, why it’s important to protect it, and common-sense safeguards. Originally, this training was mandatory for the adult members, and if they did not complete it by the deadline, they were suspended from participating in operational missions. Later, this requirement was extended to the cadet members of CAP as well, based on the facts that some older cadets participate in the operational missions, and they were all in an environment where they could learn details of the operational missions easily.

Most missions of Civil Air Patrol and other semi-official organizations like the Coast Guard Auxiliary handle missions that involves unclassified information that is designated For Official Use Only (FOUO). This information can be processed and stored on unclassified computers and transmitted via e-mail, even across the Internet. This is the common method for communication between government agencies and the volunteer organizations they reach out to for support. Because of CAP’s unique relationship with the Air Force, they have the ability to work, when required, on more sensitive information due to their access to military installations and operations centers.

Through a combination of technology, policy and screening process, volunteer and auxiliary organizations can be a tremendous force multiplier in this era of high operational tempo, stretched resources and an entirely new type of threat and mission profile. Before reaching back to these resources, agencies need to think through their next generation of information security.

[MK adds:

Non-volunteer and non-governmental organizations can learn from the experiences of the CAP and other volunteer agencies. Today’s environment requires even more attention to the
background of potential employees and even of visitors. For example, instead of automatically accepting all the details of an applicant’s résumé, the human resources department can make a point of checking on the accuracy and completeness of details of that record. Are the dates correct? Are the positions accurately named? Did the references named in the document agree to be references? What do they have to say about the applicant?

Similarly, visitors to high-security areas should be vetted before granting access. Is that journalist who requested an interview with the data-center manager really a journalist – or is (s)he an industrial spy or a hacker using social engineering? Is the salesperson claiming to be from MegaCorp really representing that company – or trying to sneak through your security barriers on behalf of a competitor?

You remember the old adage, surely: TRUST, BUT VERIFY!

* * *

Lt Col Robert Jennings is a senior volunteer in Civil Air Patrol. He is heavily involved in the cadet program and is highly qualified and experienced in CAP’s homeland security and counterdrug missions as an aircrew member. After military service in the late 1970s through the mid 1980s, he has been in the technology industry for more than 20 years, working on several government IT projects for agencies that include the Department of Defense, FBI and the former Immigration and Naturalization Service. He currently works for Dell, and his technology specialties include messaging and collaboration, security and identity management. He can be reached at <mailto:Robert.Jennings@njwg.cap.gov>.

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>  

Copyright © 2009 R. E. Jennings & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.