Information Security and the Outsider:
Part 1 – The New Government INFOSEC Environment

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

In a world of new, unconventional military conflict around the globe, one of the largest producers of secure information, the U.S. Government, has had to create non-traditional partnerships to help accomplish domestic missions. In this two-part series, guest writer Lt Col 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 part 2, he provides a case study of how one of those organizations adapted to provide better information security for their new assignments.

The remainder of these columns is entirely Lt Col Jennings’ work with minor edits.

* * *

The world has changed radically since the end of the cold war in the early 1990s. In the United States, our military and other security agencies have been challenged by extensive military operations in Iraq, Afghanistan and many smaller global hotspots. More than 50% of the National Guard has been deployed since 2002 in support of these campaigns. Many domestic emergencies and assignments that traditionally would have been responded to by the National Guard in individual states need an alternative resource.

One of the outcomes of all this change is that the military, Federal Emergency Management Administration (FEMA), Homeland Security, the Coast Guard and other government agencies reaching deeper in to the ranks of non-traditional human resources such as auxiliaries and non-governmental organizations (NGOs). In the face of all of this geo-political change, corporate change and technical evolution, we are faced with the outsider – the person outside of the organization who is not under its control, and who may not have been vetted according to usual procedures. At the same time, this outsider is critical to the agency’s success, because these outsiders are volunteers.

Volunteer organizations like the Red Cross, Civil Air Patrol, National Association for Search & Rescue (NASAR) and dozens of secular and faith-based organizations have been a critical component of disaster relief and search and rescue for decades. These operations rarely involved information that could be considered sensitive. Today, however, volunteers may have access to or even depend on sensitive information as they contribute critical services.

Further complicating all of these fundamental shifts are the advances in technology that simultaneously make information easier to and harder to distribute. Advances in protecting information inevitably trail the innovation in sharing it. The Internet is the fundamental catalyst of all of this change, but even hardware like digital cameras and USB storages devices smaller than a thumbnail make information more transportable and more difficult to protect than ever.
before. Often, as technological innovation emerges, we cannot envision the consequences it will ultimately present.

All of this technology only enables the sharing of this information – people are the ones who actually do the sharing (or, in some cases, stealing). We look to technology solutions to protect this information but forget that policy, process and training are all critical factors in the protection of information.

Vetting volunteers offers lessons to all organizations, even those that don’t use volunteers, on how to cope with the increasing operational security requirements of today’s environment.

* * *

In the next part, Lt Col Jennings will look at how both the Civil Air Patrol and the US Government adapted their information security policies and practices to interoperate effectively in the new threat environment.

* * *

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.