Berlin Address: 22 May 2014

Aviation-Risk-Based Security: A Way Forward through Improved Understanding of Collaboration, Cyber Security, and Information Sharing

By Dr. Robert A. Hickey, Deputy Director
ODNI/Air Domain Intelligence Integration Element
May 22, 2014

Thank you (whoever introduces), and thank you all for the opportunity to be here today to talk about aviation security.

As everyone here knows, aviation is a cornerstone of global transportation and therefore global commerce. An interruption of air service for any global business would have a catastrophic impact. The purpose of the Office of the Director of National Intelligence-Air Domain Intelligence Integration Element (commonly referred to as the Air Element) is to enhance the safety and security of the global air domain. The Air Element represents the Director of National Intelligence (DNI) and serves as the Intelligence Community's primary national-level representative for aviation-related intelligence integration and information sharing issues. Our vision is a nation whose air domain is more safe, secure, and resilient as a result of the intelligence- and information-sharing activities of the Global Air Community (GAC).

Allow me a moment to define some terms, specifically what we mean when we refer to the air domain, air domain awareness, and the Global Air Community.

> The **air domain**, as defined by the US National Strategy for Aviation Security, is "The global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating, and people and cargo present in that airspace, and all aviation-related infrastructures."
>
> **Air domain awareness** is "the effective understanding of threats associated with the Air Domain that could impact the security, safety, or economy of the United States."
>
> The **Global Air Community** is "the Federal, State, tribal, and local departments and agencies with roles and responsibilities in the Air Domain including all the public, private, and international stakeholders."

Actors, Tactics, and Targets

Now that I have defined these three terms, I would like to focus on the actors threatening the air domain and their tactics and targets. The 2009 U. S. National Aviation Security Policy stated that threats to the air domain emanate from three sources: hostile nation-states, terrorists, and criminals. These actors seek to use the following tactics against aircraft and its infrastructure: hijackings, bombings, shootings, smuggling/conveyance, and cargo crimes (contraband, theft, etc.). Their targets include large passenger aircraft, large all-cargo aircraft, small aircraft, and nontraditional aircraft, such as unmanned aero vehicles (UAVs), aviation transportation system infrastructure, and air cargo.

According to a speech given by TSA Administrator John Pistole to the American Association of Airport Executives in December of 2011, the aviation industry's approach to threat actors changed dramatically following the terrorist attacks of September 11, 2001. Prior to the 9-11 terrorist attack:

- No cohesive system in place to check passenger names against terrorist watch lists in advance of flying;
- Only limited technologies in place for uncovering a wide array of threats to passengers or aircraft;
- No comprehensive federal requirements to screen checked or carry-on baggage;
- Minimal in-flight security on most flights; and,
- A lack of timely intelligence-sharing in both directions: from the federal level down to the individual airports, as well as from an individual airport up to the national level.

Then the United States was attacked on 9/11, and everything changed. Americans came to understand what those of you in the industry knew instantly: that air travel would never be the same (Pistole, 2012, Para 11). This event made clear to any doubters that aviation is

inherently vulnerable to a variety of threats. The dynamic nature of the Air Domain creates an environment that is vulnerable to bad actors seeking to conduct so-called "spectacular" attacks, and also difficult to defend. In the simplest of terms, the best aviation security solution would be to keep bad things and bad people away from airplanes and airplane-related infrastructure and people. Regrettably, it is virtually impossible to protect against every potential threat to aviation.

The Need for Collaboration—and Vulnerability

For the next few minutes I would like to focus on a fundamental element of aviation security: collaboration. Then I want to draw your attention to what is likely to be a future threat to the aviation: its operational dependency on information systems technology, or cyber.

The need for information sharing, especially security-related information, within the Global Air Community has never been more acute. Let me illustrate this point with an example. If analysts had examined the data prior to the 9-11 terrorist attacks, they might have found it highly suspicious that the terrorists were practicing takeoffs rather than landings. Every aviator knows that landings are much more complicated and require much more practice than takeoffs. This information, gained through a collaborative network, might have focused analysts' attention on the terrorists' plot. Viewing issues from an aviator's perspective is invaluable to enhancing the security of the Air Domain. Ms. Coleen Rowley, FBI Minneapolis Field Office legal counsel and special agent, made this point in her testimony before the Senate and the 9-11 Commission.

If the Global Air Community is going to make strides to secure the global Air Domain from future attacks, members of this Community—including public, private, and international stakeholders—will need to share information with each other. Government and industry must develop robust transparency policies that include academia. Although information sharing is not an easy task, the benefits of cooperative and

transparent collaboration—which is to say, safer air travel—far outweigh the costs. How should members of the Global Air Community collaborate?

The best solution is by leveraging information technology—especially virtual collaboration tools. Such tools are especially important to industries that are physically distributed, such as we have in the international aviation industry. Research demonstrates the potential to advance the effectiveness of teams and reduce friction and misunderstanding during business mergers by employing virtual collaboration tools. Studies also (Kehoe, 2011) demonstrate a positive correlation between collaboration and increased mission capability and performance. This concept of virtual information sharing can be employed and leveraged within the Air Domain to increase our opportunities to prevent bad things from happening to airplanes and related infrastructure. In aviation security, the types of insights that this collaboration could generate has a real potential to save lives.

While virtual collaboration and information sharing within the aviation industry is a proactive step we can take, there are also precautionary measures which should be considered prior to enhancing the online information sharing environment. Today's aviation industry already depends upon technology to collaborate and communicate. If not properly secured and monitored, this technology and data could be vulnerable to cyber attacks. The sensitive data contained on aviation industry information technology systems may be vulnerable to exploitation by hostile nation-states, terrorists, and criminals. Inevitably, systems connected to the World Wide Web are not safe, and the data contained in those systems are also not safe. A virtual aviation industry collaboration space would therefore need and aggressive cyber security plan to reduce the likelihood of cyber attacks and data leaks.

Cloud computing technology may be a partial solution to the information systems security problem that a virtual information sharing platform may encounter. By reducing the number of attackable data

sources, one can reduce the number of target opportunities. However, even isolated stand-alone systems are at risk from insider threats (Cappelli, Moore, Trzeciak, & Shimeall, 2009; Yang & Wang, 2011). Insider threats can be discouraged through training programs and end user policies, however, studies indicate that achieving 100% effective information assurance is impossible (Bodin et al., 2008).

As a Global Air Domain community we will have to address what level of risk we are willing to accept regarding information leaks and theft. Will the opportunity we gain to save lives and mitigate potential threats through information sharing and collaboration be worth the risk of cyber attacks or insider threat-related data leaks? Is passenger and crew safety worth the risk?

Aviation-related IT systems will not be, and are not, immune to vulnerabilities, but I assert that we can manage the risks. (Chen, Kataria, & Krishnan, 2011). Leaders in the aviation industry must assess the risks associated with using their systems and move toward plugging the biggest holes or assessing the perceived composite risk (Ekins et al., 2012).

One of the most significant threats to aviation security-related information systems will very probably be insiders (Yang & Wang, 2011). Policies cannot prevent an employee who is authorized to use a system from damaging the system if they have the intent to do so. Profiling an individual employee prompts civil liberties questions which will vary by country, and therefore obfuscate the issue further (Posner, 2009; Schwartz, 2009).

The debate surrounding information security policy and civil liberties is vigorously argued on a global scale. Due to the international nature of the Global Air Domain, these debates will impact the establishment, and ultimately the level of success, of a virtual information sharing platform for the aviation industry.

Information security innovation must address the various aspects of information security, policy, risk, technology, business priority, and end-user awareness and compliance (Li et al., 2012; Puhakainen & Siponen, 2010; Siponen & Vance, 2010; Team, 2012). Wright and Wright (2002) conducted an exploratory study designed to understand the unique risks associated with the deployment of an enterprise resource planning system (ERP). An ERP consists of a system of systems not unlike the multitude and complexity of systems on modern airliners today, and, as such, there is the risk at every level of deployment (Wright & Wright, 2002). The larger or the more complex the system, the greater the information security risk to the system. Wright and Wright noted that ERP implementation is fraught with a significant risk from inadequate business-process impact consideration. Additionally, they explained the inadequate business-process impact considerations translate into increased risk that different vendors pose as an organization purchases component IT solutions or products.

Considering the complexity of the system of systems associated with modern airliners, traditional defense strategies; hardware and software; changes to policy or governance; and end-user training will not stop tomorrow's IT attack. As we are all acutely aware, such an attack would be disastrous in aviation.

So one might ask, what is the solution or how do we solve the problems with aviation security and in particular the emerging potential of the IT threats we are only beginning to consider? The answer to this question may lie in a crowd sourcing collaboration solution, currently being studied by the Intelligence Advanced Research Product Activity (IARPA). Innovation in a particular area may be found in an entirely unrelated discipline. Posing a question, or presenting a problem to a disparate group of people, a crowd, who could collaborate with each other and leverage different suggestions may prove effective in difficult issue problem solving. As we venture into the possible unknowns of threats to aviation, to include unknown IT threats; crowd sourcing and

collaboration may prove fruitful in identifying solutions, and beneficial in developing the right questions that we are yet to consider.

Collaboration, in many different forms, leverages IT as a force multiplier in government and business. Protecting and using IT in aviation is critical as the global economy continues to shrink the size of our planet. We can ill afford not to reach across national boundaries to work positively for the good of all, we must collaborate. We must begin to look forward to discovering the questions to secure our aviation industry, questions that we have not even thought to ask yet.

Thank you all for your attention.

Berlin Address: 22 May 2014

References

Bodin, L. D., Gordon, L. A., & Leob, M. P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64-68. Retrieved from http://www.rhsmith.umd.edu/faculty/mloeb/Cybersecurity/Information%20Security%20and%20Risk%20Management.pdf

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. (2009). *Common sense guide to prevention and detection of insider threats* (3rd ed.). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Retrieved from http://www.cert.org/archive/pdf/CSG-V3.pdf

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly, 35*, 397-393. Retrieved from ezproxy.apollolibrary.com/ehost/results?sid=e3c7eef3-96f3-43ac-a6b5-7bdaae20aff7%40sessionmgr110&vid=6&hid=127&bquery=Chen%2c+P.%2c+Kataria%2c+G.%2c+%26+Krishnan%2c+R.+(2011).+Correlated+failures%2c+diversification%2c+and+information+security+risk+management.+MIS+Quarterly%2c+35%2c+397-393.&bdata=JmRiPTI3aCZkYj1hOWgmZGI9YXdoJmRiPWFobCZkYj1xYmgmZGI9YnRoJmRiPXJ6aCZkYj11ZmgmZGI9aWloJmRiPWkzaCZkYj1lb2gmZGI9ZWhoJmRiPTIwaCZkYj0yNmgmZGI9OGdoJmRiPWhqaCZkYj0yMmgmZGI9bGtoJmRiPWY1aCZkYj1tbmgmZGI9bjJoJmRiPXRmaCZkYj0yMWgmZGI9YndoJmRiPWU2aCZkYj1lMGgmZGI9c2loJmNsaTA9RlQmY2x2MD1ZJnR5cGU9MCZzaXRlPWVob3N0LWxpdmU%3d

Ekins, J., Peters, S. M., Jones, Y. L., Swaim, H., Ha, T., La Neve, F., . . . Yancy, H. F. (2012). Development of a multiplex real-time PCR assay for the detection of ruminant DNA. *Journal of Food Protection, 75*, 1107-1112. doi:10.4315/0362-028X.JFP-11-415

Kehoe, B. (2011). Progress report. Qaulity measurement tools and expanding collaboration drive success. *Health Facilities Management, 24*(12), 27-30.

Li, C., Peters, G. F., Richardson, V. J., & Weidenmier Watson, M. (2012). The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly, 36*, 179-204. Retrieved from http://misq.org/the-consequences-of-information-technology-control-weaknesses-on-management-information-systems-the-case-of-sarbanes-oxley-internal-control-reports.html

Posner, R. A. (2009). National security and Constitutional law: Précis: the constitution in a time of national emergency. *Israel Law Review, 43*(2), 217-224. Retrieved from http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8501839

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*, 767-764. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404809001436

Schwartz, P. M. (2009). Law and technology: Keeping track of telecommunications surveillance. *Communications of the ACM, 52*(9), 24. doi:10.1145/1562164.1562175

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*, 487-502. Retrieved from http://www.misq.org/skin/frontend/default/misq/pdf/appendices/2010/SiponenVanceAppendices.pdf

Team, V. R. (2012). 2012 data breach investigations report. *Verizon Corporation.* Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?__ct_return=1

Wright, S., & Wright, A. (2002). Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems Education, 16*, 99-113. Retrieved from http://ehis.ebscohost.com/eds/pdfviewer/pdfviewer?sid=046efec5-6baf-4c3b-9e27-575b9b3e539b%40sessionmgr104&vid=3&hid=124

Yang, S. C., & Wang, Y. L. (2011). System dynamics based insider threats modeling. *International Journal of Network Security & Its Applications, 3*(3), 1-14. doi: 10.5121/ijnsa.2011.3301