4-2006

Contingency Planning and an Air Force Space Command Information System

Kaylin Freedman

Michael R. Grimaila
Air Force Institute of Technology

Recommended Citation

Freedman, K. and Grimaila, M.R., "Contingency Planning for an Air Force Space Command Information System," High Frontier Journal, Vol. 2, No. 3, Apr. 2006, pp. 76-81.

Contingency Planning and an Air Force Space Command Information System

Maj Kaylin Freedman, USAF
Michael R. Grimaila, PhD, AFIT

It is a quiet afternoon. You are sitting in your office thinking about how many wings in Air Force Space Command (AFSPC) utilize electronic databases to enter and track operational training, evaluation, and Crew Force Management (CFM) data. This data directly supports the missions of the units by meeting regulatory requirements to maintain proficiency and qualifications, ensuring only personnel meeting the physical requirements perform shifts, determining crew member proficiency for advancement within the unit, and enabling analysis of data to improve operations. No single, common system is in use across the command. The databases in use are not consolidated or standardized and do not interface. This is not efficient and a new system would offer advantages.

You look out the window and envision the accolades you will get if you propose a single, common training, evaluation, and CFM information system and wonder what leadership could possibly fear about a proposal such as this one. Suddenly the phone rings, the site administrator for your single, common information system is on the line wanting to know if you have seen the news and would like your opinion on what to do next. Every phone line in your office starts ringing. Your flustered assistant runs in. You do not know what to do. You put everyone on hold as your assistant explains that a tornado has touched down in Colorado Springs. The building that houses the servers for your system for the entire command was destroyed. The loss of the system means that eight wings and one group, comprising 38 operational units, will have to spend an unspeakable number of man-hours to reproduce, to retrain, and possibly re-evaluate over 3,000 operators. Even worse, a data loss could compromise the weapon systems because without the data the units would no longer know who is physically and proficiency qualified to perform a shift. For the three Intercontinental Ballistic Missile bases, this means a nuclear surety incident could occur which would result in a reduction of alert rate for the first time in over 50 years. As you are thinking about what this means for AFSPC and the country, the commander enters your office. You know the commander is looking for answers, but you simply stare speechlessly. Every minute that ticks by you know the units are falling behind, nuclear surety is possibly compromised, and precious manpower is being wasted. The commander is furious and tells you to grab a box and start packing.

The phone rings again, and you realize you were daydreaming. There is no crisis, but now you realize that leadership might resist your idea of a single, common training, evaluation, and CFM information system because of the risk of losing the data due to a contingency such as a natural disaster. So, before you start a proposal for AFSPC, you decide to examine what is necessary to reduce the risk associated with a critical information system and contingencies.

Overview

Building contingency plans calms fears regarding potential losses of information systems which are critical to an organization and vital to the operation's continued success in a time of crisis; the drama demonstrated above provides just some of the results of not planning ahead. For the purposes of this discussion, the focus of the contingency planning is mainly on the impact to information systems and not the impact on people. Although the impact on people is important, military units are required to maintain disaster preparedness plans which already focus on what steps leadership and subordinates should take during disasters to assist with personnel requirements such as first aid, and assembly points. The term "contingency" refers to an event which makes usage of an information system, asset or process, not possible for a period of time or permanently. A contingency does not include an event which precludes usage of an information system as a result of a security issue such as a compromise or malicious attack.

This article will illustrate that a contingency plan reduces risk by examining the impact on civilian organizations and providing examples from 11 September 2001. We then examine the purpose of risk assessment and a technique for conducting risk assessment. A planner cannot properly design a contingency plan until the risk and potential losses are determined because these factors establish the need for a plan. Finally, we provide a guide for constructing a contingency plan. The planner must adhere to a guide to build the plan in order to ensure that it encompasses what is necessary for survival and to ensure the plan is thorough. This article is not all-inclusive, and it is important to note there are a variety of approaches to contingency plans and procedures; the purpose here is to highlight the importance of developing and using a contingency plan and to provide an insight into the overall process of contingency plan construction.

Why Contingency Plans Are Critical

The role of information and the systems providing the information in today's society are vital. The vast majority of organizations would not be able to function without information, and if information were lost, it could be detrimental to operations. In 2000, Price Waterhouse Coopers reported "that 90 percent of all companies that experience a computer 'disaster' with no pre-existing survival plan go out of business within 18 months."[1] The survival rate of organizations without

a pre-existing contingency plan seems extremely low, and Price Waterhouse's data would be suspect if other institutions did not report similar results. However, the Hartford Insurance Company found that "on average, over 40 percent of businesses that do not have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm."[2] Gartner Dataquest further substantiated the findings by reporting that "two out of five enterprises that experience a disaster go out of business within five years."[3] Organizations that understand the criticality of contingency plans devote the necessary resources to ensure they are available when needed. According to Donna Scott, a consultant with Gartner Group, banks expend seven to eight percent of their data center budgets on disaster recovery.[4] The number of organizations predicted to fail due to a contingency are astounding, and the amount financial institutions expend on contingency plans highlight the importance of having a solid plan in place.

Unfortunately, 11 September 2001 illustrated why contingency plans are critical. Due to the visibility and the centralization of financial institutions in the World Trade Center, their destruction and the impact widely increased the impact of the desolation. Many companies could not function for days while others were able to return to operations within hours. Deutsche Bank had to evacuate over 5,000 employees, and lost offices and all equipment, but were operational within two hours. A bank spokesperson said, "Our plans worked well, our systems came back up; we were well prepared."[5] Unfortunately, others were not as lucky.

The most significant and common technology failure was the loss of telecommunication. This factor severely hampered disaster recovery for many organizations: "Two major Verizon points-of-presence were located in the World Trade Center complex, and damage was also sustained by a nearby switching unit."[6] Organizations attempting to restore operations and who relied on telecommunications for data transfers and customer support were severely hampered by the reduction in capabilities. An additional crippling factor was the lack of redundancy. Todd Gordon, vice president and general manger for business continuity and recovery services at IBM, said, "There was too much concentration of traffic over networks at one Verizon site" and added that organizations will "require greater redundancy in telecommunications and networking in the future."[7]

Another issue that companies experienced was the complete loss of systems and vital information infrastructure. This caused significant and challenging problems: office space had to be secured, equipment located, and systems built. Leslie Hunt, chief information officer of the Greater New York chapter of the Red Cross, highlighted the importance of having plans in place to establish systems for people to use. Her office had lost everything, and had no plan for how to obtain equipment. Hunt was able to secure 12 computers, create local area network and wide area network, and proceed to work on making the e-mail servers function.[8] However, without a plan, the cannibalized system was fragile and vulnerable. The computers and network were not properly configured and, in the end, could not handle the workload. The Greater New York Website crashed several times and a virus infected the e-mail server, making the systems inoperable for a period of time.[9] For the survivors of 11 September, the Red Cross provided an essential source of information, and without the website and e-mail the Red Cross was crippled. Hunt pointed out the need to have plans which ensure the systems are in place during a disaster so that people can do their jobs "without having to worry about the technology they are using."[10]

Risk Assessment

When the organization is undergoing a contingency, it is not the time to try to determine what information systems are the most critical. In order to avoid this, organizations must conduct a risk assessment prior to a contingency plan being composed or in concert with the initial steps. The assessment should entail determining the organization's assets and processes, assigning a value to the assets and processes, identifying possible contingencies the organization faces, and assembling a detailed report which provides recommendations for building the contingency plan. The risk assessment will ensure the need for a contingency plan is determined before manning is expended on drafting one, and a risk assessment will also ensure the focus of the plan is on the systems the organization has assessed as critical to the organization's operations. A planner can conduct risk assessment or management in a number of ways. The methods are very similar and serve the same goal of helping the organization understand, manage, and reduce the risks encountered in conducting their mission. The process described here is based on the steps highlighted by Michael Erbschloe, author of "Guide to Disaster Recovery." Figure 1 displays the steps involved:

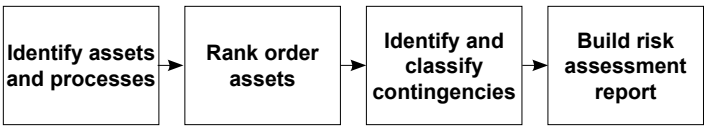

Figure 1: Risk Assessment Steps.

One of the first steps of risk assessment is to identify what assets the organization possesses and the processes used to conduct operations. This means conducting an inventory of every piece of equipment the organization has and documenting the processes that the organization accomplishes in order to fulfill its mission. Erbschloe suggests an organization conduct an exposure inventory which lists "all facilities, processes, systems, and resources that an organization uses to maintain operations and sustain revenue" and includes physical facilities, personnel, equipment, installed systems, information technology, office equipment, and products or parts.[11] Once the equipment is identified, the organization must be aware of how the inventory is used so that during a contingency the right equipment is made available to the right people so the right tasks are accomplished to ensure continued operations. Erbschloe identifies this as the "business processes inventory" and clarifies that it must include: "how a process works, the facilities and buildings in which the process occurs, the departments that perform the process, the personnel who work in the departments, the equipment used by the departments, the installed systems on

which the departments rely, the information technology that the departments have in place, and the parts and supplies that the departments need to accomplish their work."[12]

Once planners know what assets are in the organization, they need to know which ones require the most protection. The organization must carefully rank order its assets. During a crisis, people should not spend valuable time determining what equipment is critical to operations and what should be saved. Determining the value of systems in the military can be problematic because there is no profit affected and sometimes no identifiable customer impacted. The planner for a military unit needs to assess the value of the assets or processes based on support to the mission. Can the mission be accomplished without the asset or process? If not, the value is high and the asset or process should earn the highest value of 10. If the answer is yes, the planner must determine at what point the asset or process *does* affect the ability of the unit to perform the mission and assign a value based upon this assessment. According to this model, the greater the number of hours between the assets or processes inoperability and the resulting impact on the mission then the lower the value (determining the spread of the size of the value awarded would be contingent to the number of assets and processes). In other words, a system which would impact the mission in eight hours if the system is not operable would garner a value of eight, whereas a system which would impact the mission in 16 hours if the system is not operable would be given a five.

Once the assets and processes at risk are identified and the value is known, the planner must list and classify the possible contingencies. Peter G. Neumann, moderator of the online ACM Risks Forum, noted that organizations, especially governments, build plans to meet the situations of the past instead of designing plans to meet the potential new situation.[13] One way to avoid this trap is for the planner to ensure all contingencies are classified even though the utility may initially seem insignificant. Listing and classifying all possible contingencies regardless of the probability will actually improve the process by ensuring the organization is prepared for all possibilities and not just the known or most recent ones.

Michael Whitman and Herbert J. Mattord, authors of "Managing Information Security," provide a method to accomplish this task. The planner should separate natural disasters from man-made disasters and list the event followed by the suspected effect on information systems.[14] Erbschloe recommends another process of grouping threats by recurring natural disasters, accidents, and "destructive or disruptive deliberate actions" and classifying as catastrophic, major, and minor.[15] Comprehensive Consulting Solutions, however, suggests creating three different categories for classification. Category I represents the least serious threats that only last for a few hours, such as a brief loss of power. Category II consists of "localized man-made disasters and natural disasters of a more serious nature" with effects lasting for days or weeks. Category III consists of widespread events such as earthquakes or flooding with the potential to have an impact for weeks.[16]

Each of the proposed methods is adequate but when combined they provide a better picture for the planner. The planner should categorize the threats utilizing the numbering system of Comprehensive Consulting Solutions, identify the categories utilizing Erbschloe's categories, and add the suspected effect as Whitman and Mattord suggest. The resulting categories would be as follows: Category I, accidents; Category II, minor natural or human-made disasters; Category III, major human-made or natural disasters; and Category IV, widespread or catastrophic events. Part of identifying and classifying the contingencies is determining the likelihood of the event occurring. The planner must research the probability and devise a probability rating to be included for each contingency. The likelihood of a contingency occurring can be determined by contacting local agencies and conducting research on, for example, flood plains, weather patterns, fault lines, power outages, or grid construction.

Once this research is complete, the planner must tie all of this information together. Erbschole defines this activity as the risk assessment report. This consists of describing the "asset or business process that is exposed to risk, the risks themselves, and the effectiveness of existing systems designed to mitigate these risks."[17] The report is the process of compiling the first three steps described and next determining if the organization's procedures reduce or eliminate the risks identified. Initially, the planner should focus on developing a risk assessment report for the critical assets and processes. When time permits, the planner can return to this step and complete it for those assets and processes that are not as critical. Completing this step and moving to developing a contingency plan should not be delayed in order to accomplish a risk assessment report on low value assets and processes.

Erbschloe also warns that a risk assessment report may contain proprietary information due to its comprehensive details, and organizations should treat the reports as confidential. The planning team will require the reports and leadership may want to review them, but minimal dissemination is ideal due to the detailed content.

Building a Contingency Plan and Beyond

After the planner has assessed risk, the actual contingency plans can be written. A number of different methodologies for writing plans exist and most of them are very similar. "Management of Information Security" presents a comprehensive and usable contingency plan model. This model leads the planner through a logical procession from a minor contingency, to a major, to a catastrophic and describes how to construct plans to address each type. What follows is a broad overview of the model.

According to "Managing Information Security," the contingency plan consists of three components: the incident response plan, the disaster recovery plan, and the business continuity plan. An organization must develop each component for each category of contingency identified during the risk assessment phase. This will ensure that personnel are clear on the required steps and procedures to take during a contingency. As William A. Hussong, Jr., the senior member of the professional staff of the special operations division of System

Research Applications, Inc., explains, "The plan must basically outline people's responsibilities, the use of equipment and other material resources, and detailed operating instructions; nothing can be assumed. The plan is the organization's strategic battle plan for recovery… [and the components] …become the organization's tactical battle plans for survival."[18]

The first, and the largest, component of the contingency plan is the Incident Response Plan (IRP). This is a reactive measure that "comprises a detailed set of processes and procedures that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and assets."[19] It is the starting point for all events and includes a set of procedures for personnel to follow. If at all possible, a contingency should be contained and kept at what was defined as the minor - Category I or II - level with the goal to address it before it becomes a major event. To accomplish this task, the incident response plan must detail the procedures for personnel and the organization to take during, after, and before a contingency occurs. The actions taken are function-specific and are grouped and specifically assigned to individuals.[20]

The IRP is the first component of a contingency plan, and a Disaster Recovery Plan (DRP) is the second. This plan is enacted when a natural or human-made event occurs in which the organization cannot control the impact of an event or the level of damage is so severe that the organization cannot quickly recovery.[21] The DRP plan focuses on preparing for a disaster so that restoring operations and recovery is quickly possible. The plan must address all category levels of contingencies identified during the risk assessment phase. However, the planner must understand that even though the major and catastrophic contingencies - Category III and Category IV - have a lower probability of occurring, they can have the most overwhelming impact to an organization.

The key points of the DRP are "clear delegation of roles and responsibilities," "execution of the alert roster and notification of key personnel," "clear establishment of priorities," "documentation of the disaster," "inclusion of action steps to mitigate the impact of the disaster on the operations of the organization," and "inclusion of alternative implementations for the various systems components, should primary versions be unavailable."[22] The DRP focuses on restoring normal operations to the organization as quickly as possible and includes crisis management steps. The crisis management actions are those "that deal primarily with the people involved" and comprise of detailing public affairs responses, handling emotional issues, and verifying personnel status.[23] The disaster recovery plan prepares the organization to restore operations when the primary operating location is still intact.

When a contingency is so catastrophic that an organization is unable to operate out of its primary location, then the last component of the contingency plan, the Business Continuity Plan (BCP), must be enacted. This plan includes the strategies to ensure the company can continue to perform its mission and continue to function during a contingency, regardless of the magnitude, and is usually managed by the leadership.[24] The BCP is critical because an organization must continue to perform its mission or the organization risks going out of business, which for a military organization could impact the security of the entire nation or worse. The key here is developing plans to ensure the most mission critical assets or processes are able to continue to function or to ensure they can be quickly restored regardless of the occurrence of a contingency.

Restoring assets and processes is possible by taking pre-contingency actions to protect the information. Accomplishing this serves several purposes such as ensuring that data critical to the organization's mission is available, guaranteeing facilities are available, and reducing risk. The organization should conduct pre-contingency actions on those high value assets and processes identified in the risk assessment phase.

As mentioned above, the organization's assets and processes were ranked based upon their value to mission performance. The planner used this information, budgetary constraints, and acceptable risk levels to evaluate which options work best for contingency. Six available options are suggested: hot site, warm site, cold site, timeshare, service bureau, and mutual agreement. The first three options are "exclusive-use" (only the organization can use the site) and the remaining options are shared-use. "A hot site is a fully configured computer facility, [and it has]…all services, communication links, and physical plant operations" available.[25] Although this option is expensive, it provides instant recovery of data and operations can continue almost seamlessly (assuming the hot site is not also impacted by the contingency). The next option is a warm site which "provides many of the same services and options as the hot site, but typically software applications either are not included, or are not installed and configured."[26] Finally, a cold site, the least expensive option, consists of "only rudimentary services and facilities" and is essentially "an empty room with standard heating, air conditioning, and electrical services."[27]

Shared-use options, unlike exclusive-use, mean that the organization shares usage of the facility or services with another organization. The timeshare option can be a hot, warm, or cold site, "but it is leased in conjunction with a business partner or sister organization."[28] Success is contingent upon the partner or sister organization's cooperation and adherence to the timeshare agreement. A service bureau can be employed and is "a service agency that provides a service for a fee" such as data storage or floor space.[29] The final option is the mutual agreement which "is a contract between two organizations in which each party agrees to assist the other in the event of a disaster."[30] An organization chooses which option is right for them based upon what expense it can support, what level of risk it is willing to accept, and the timeframe of desired operational recovery.

All of the options require the ability to access the organization's data, information systems, and processes in order to operate. There are three different methods of storing or protecting the data, information systems, and processes. One of these is electronic vaulting: "the bulk batch-transfer of data to an offsite facility."[31] The organization periodically conducts a batch-transfer of data to a server at another location. Except that the server is located off site, this is similar to a traditional back up; the data is only as current as the latest transfer. Remote journ-

aling, another option, transfers "live transactions to an off-site facility" so the transaction is current, but it does not transfer the archived data.[32] The last and most comprehensive option is data shadowing which "combines electronic vaulting with remote journaling, by writing multiple copies of the database simultaneously in two separate locations."[33] Although data shadowing is expensive, it is the most thorough, will reduce the time required to recover operations, and ensures profit loss and mission impact is minimal.

Once the planner writes the contingency plans, they must be tested and updated on a regular basis to ensure currency, accuracy, feasibility, and applicability. Although many organizations affected on 11 September had contingency plans, many were not usable. A consultant at Strohl Systems, a recovery software and services firm, explained that "in some cases, the plans were too big and ignored detailed issues-where to meet, how to contact people, having a disaster hotline that works when all phone systems are down."[34] The senior vice president of field operations at Comdisco, a contingency services provider added, "We found that [during the events of 11 September] our clients were for the most part undersubscribed in terms of their need for contingency work areas and networks and terminals…Plans need to be updated every six months."[35] Hussong, the senior member from System Research Applications, Inc., however recommends rewriting contingency plan procedures at least every five years to ensure requirements are kept current, new technologies are utilized, and "fresh eyes…look at old solutions to new problems."[36]

The actual contingency plan must be available during a contingency. As one firm discovered during 11 September, the only copy of the contingency plan was located in the World Trade Center offices, and at another organization, said Strohl Systems' Banker, "they had copies of the recovery plan on the network in New York and London and Tokyo, but they could not get to any of them [due to the lack of telecommunication]."[37] However, there is a difficult balance to maintain between availability and protecting the organization. To ensure the plan is available accessible, organizations must have multiple copies of contingency plans available as hard copies, on different networks, and even on multiple hard drives. However, due to the proprietary issues and other classifications issues, the organization must be careful not to broadcast the plan to uncontrolled locations. This is an essential point for the planner to keep in mind as they disseminate the completed plan to the personnel in the organization.

Option For Air Force Space Command

A single, common training, evaluation, and CFM information system for all of AFSPC would be subject to risk from a contingency just like any other system. However, if risk assessment is conducted and a contingency plan is built AFSPCs leaders could accept the risk of a contingency occurring.

One way to immediately reduce the risk of a contingency is to wisely choose the location of the database server based upon what was learned about contingency plan building. Utilizing the Air Force's Global Combat Support System (GCSS) is one way to apply this knowledge. According to the Warfighting Integration and Chief Information Officer, Knowledge Information Management Branch at Headquarters Air Force, the GCSS provides a central enterprise server bus to house data that permits authorized users access via remote sign on; it is a set of enterprise information services and is protected by multiple layers of security.[38] Defense Information Systems Agency (DISA) is responsible for parts of GCSS. DISA hosts GCSS on a server farm located in Alabama with data shadowing occurring with a server farm at Wright Patterson AFB in Dayton, Ohio. There is a third server farm proposed for San Antonio, Texas which will have the same data shadowing service. Data and transactions will therefore be stored in three different geographical locations, significantly reducing risks. AFSPC users would access the single, common information system via remote sign on through the Air Force Portal Graphic User Interface.

Housing the database on the GCSS is only one way to reduce the risks associated with this system and will increase leadership support. A full risk assessment and contingency plan would need to be accomplished in order to further mitigate the risk to an acceptable level.

Conclusion

Without contingency plans, organizations risk not being able to survive or experience mission failure. Contingency plans help an organization to determine what risks they are willing to accept and what risks are unacceptable, providing the opportunity to take actions to mitigate unacceptable risks. Using examples of what organizations experienced during 11 September, we have illustrated why a contingency plan is critical. As highlighted, the loss of capabilities for organizations without a plan or those with untested plans is devastating. Before a contingency plan can be initiated, a risk assessment must be accomplished as it identifies the assets and procedures that are important to the organization, attempts to determine types and chances of a contingency occurring, and assigns a value level to the asset or process so the organization knows where to focus its efforts. Only after this has occurred can a contingency plan be built. A number of different approaches exist to build a contingency plan. The blueprint presented here is a logical and thorough method. An incident response plan is designed to establish procedures to deal with the event immediately. A disaster response plan is the next step. This will ensure there are procedures available if the contingency cannot be contained with the incident response plan. The last plan to be designed is the business continuity plan which ensures the organization can restore operations if the contingency renders the primary site unusable. With the contingency plan, comprised of these components, an organization is prepared to successfully face almost any risk.

Armed with this information, an organization will be able to face a contingency and survive. Now you can stop staring out the window and begin to effectively address some of leaderships' possible concerns regarding the implementation of a single, common training, evaluation, and CFM information system and finally make the dream a reality. Each of us has a

responsibility to contribute to the survivability of their organization. Can your organization survive a disaster?

Notes:

[1] Andy S. Krupa, "The Oversight of Physical Security and Contingency Planning," SANS Institute (2003), 1.

[2] Michael Whitman and Herbert J. Mattord, *Management of Information Security* (Canada: Course Technology, 2004), 65.

[3] Parveen Bansal, "Ministers of Information," *The Banker* 151 (November 2001) 92-93.

[4] Johannah Rodgers, "A Sense of Urgency," *Bank Systems & Technology* 38 (7 December 2001) 32-34.

[5] Ibid., 32.

[6] Ibid., 33.

[7] Ibid., 33.

[8] Matthew Vilano, "9/11: A Lesson in Crisis Control," *TechRepublic*, 21 December 2001, http://www.techrepublic.com (12 November 2005).

[9] Ibid.

[10] Ibid.

[11] Michael Erbschloe, *Guide to Disaster Recovery*, (Canada: Course Technology, 2003), 52.

[12] Ibid., 58.

[13] Peter G. Neumann, "Anticipating Disasters," *Communications of the ACM* 48 (Mar 2005), 128.

[14] Whitman and Mattord, *Management of Information Security,* 77-78.

[15] Erbschloe, *Guide to Disaster Recovery,* 62, 137.

[16] "Defining what Types of Disasters Need to be Planned for," Comprehensive Consulting Solutions, Inc., March 2001, http://www.compsoln.com (11 November 2005).

[17] Erbschloe, *Guide to Disaster Recovery,* 64.

[18] William Hussong Jr., "So You're the Company's New Contingency Planner!," *Disaster Recovery Journal*, http://www.drj.com (12 November 2005).

[19] Whitman and Mattord, *Management of Information Security,* 67-68.

[20] Whitman and Mattord, 68-69.

[21] Whitman and Mattord, 77.

[22] Whitman and Mattord, 79.

[23] Whitman and Mattord, 80.

[24] Whitman and Mattord, 82.

[25] Whitman and Mattord, 83.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Whitman and Mattord, *Management of Information Security,* 84.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Rodgers, "A Sense of Urgency," 32.

[35] Rodgers, 33.

[36] Hussong, 2005.

[37] Rodgers, 34.

[38] Action Officer, Warfighting Integration and Chief Information Officer, Knowledge Information Management Branch, Washington DC, personal meeting, 14 October 2005.

Dr. Michael R. Grimaila (BS, MS, PhD, Texas A&M University; CISSP, CISM, GSEC) is currently an Assistant Professor in the Systems and Engineering Management department and a member of the Center for Information Security Education and Research at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. Dr. Grimaila serves as Editor of the Journal of Information Assurance, Security, and Protection (JIASP), Editorial Advisory Board member of the Information System Security Association (ISSA), and is a member of the International Systems Security Engineering Association (ISSEA) Metrics Working Group. He also holds memberships in the ACM, IEEE, IRMA, ISACA, ISC2, ISSA, ISSEA, and the SANS Institute.

Maj Kaylin Freedman is currently an Intermediate Developmental Education student at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio, and is pursuing a Master in Strategic Leadership with an Information Assurance sequence, which will result in also earning the National Training Standard CNSSI No. 4012 certification. After graduating from the University of Texas, she attended Officer Training School, Maxwell AFB, Alabama. Major Freedman has served the Air Force for over 12 years in a variety of positions from adjutant to missileer to orbital analyst. Prior to her current position, she was an Operations Officer at Detachment 1, 533d Training Squadron, Schriever AFB, Colorado.