# Global Information Assurance Certification Paper

**Risk, Vulnerability Assessments, PDD 63 and Risk Management – An Overview**

Thomas P. Lardner, Jr.

The dramatic increase in computer interconnectivity and the popularity of the Internet are offering United States Government agencies unprecedented opportunities to improve operations. At the same time, malicious attacks on computer systems are increasing at alarming rates and are posing serious risks to key government operations[1]. Electronic information and automated systems are essential to virtually all major federal operations. Although they have relied on computers for years, federal agencies, like businesses and other organizations throughout the world, are experiencing an explosion in the use of electronic data and networked computer systems. As a result, agencies have become enormously dependent on these systems and data to support their operations.[2]

The United States Government is changing the manner in which it assesses the security of its operations, facilities and information infrastructure. Traditional requirements and regulations, such as Office of Management and Budget Circular A-130 Appendix III, Security of Federal Automated Information Resources, required agencies to conduct periodic risk assessments for their information systems. This was amended in February 1996,[3] after recognizing that federal agencies found it difficult to conduct effective risk assessments, the revised Appendix eliminated the requirement for formal risk assessments allowing implementation of risk management practices.[4]

Risk management is the process by which agencies or businesses make decisions regarding system operations in an effort to reduce risk to a level that ensures confidentiality, integrity and availability issues are addressed in a cost effective manner relative to the value of the information residing on a system. For risk management to be employed effectively it is imperative that decision makers are provided recommendations based on well qualified analysis of system vulnerabilities, threats and countermeasures.

In May 1998, President Clinton issued Presidential Decision Directive 63 (PDD 63). This directive tasked federal agencies with identifying the vulnerabilities to their cyber and physical infrastructure.[5] Presidential Decision Directive 63 requires agencies to approach their systems in a new way. What is your mission as it relates to the national security or the national economy? What systems, programs, or infrastructure assets support those elements of your mission supporting the national level issues? Are there interdependencies with other organizations that could impact critical systems or operations? Once these essential elements are identified the agency then has to conduct a vulnerability assessment for each target. For each target: what are

[1] Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk (GAO/T-AIMD 98-170 May 19, 1998) pg 1
[2] Executive Guide: Information Security Management, Learning from Leading Organizations (GAO/AIMD 98-68 May 1998) pg 6 URL: http://frwebgate.access.gpo.gov/cgi-bin/multidb.cgi
[3] ibid. pg 11
[4] ibid. pg 29
[5] White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998 URL: http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

the vulnerabilities, what are the threat agents which can be applied to this vulnerability, is there a credible pathway for the threat agent to meet the vulnerability, what would be the effect of exploiting the vulnerability (destruction, interrupt operations, halt the mission), are there cascade effects, does the agency have control of the threat pathway? These are just some of the issues that must be considered for each target in the conduct of a vulnerability assessment.

Identifying the vulnerabilities to an agency's cyber-infrastructure requires looking at assets in a new way. Based on my experience, the conduct of risk assessments in non-DOD agencies largely evolved into the conduct of qualitative assessments with highly limited focus. This character of risk assessments does not provide an agency or business a true picture of the viability or survivability of their information systems. Risk assessments are focused too narrowly on the potential for loss of information, interruption or denial of service, and modification of data at the system level. Often this has meant that agencies simply assess traditional access pathways, focusing on administrative, personnel, technical and physical controls specific to the system under review and the specific areas housing that system.

The conduct of a PDD 63 level vulnerability assessment takes into account the total environment to which the cyber-infrastructure is exposed. This is a much broader focus than what is described above. The findings of these PDD 63 vulnerability assessments has begun to change the way United States Government managers view the weaknesses and threats to the systems. The Department of State is bringing vulnerability assessment to the fore, based on the call within PDD 63 and the aftermath of the East African Bombings and the resulting Report of the Accountability and Review Boards.[6]

The disparity between risk and vulnerability assessments represents a flaw in the manner in which meeting federal requirements was addressed. In order to comply with a federal regulation many agencies turned assessment requirements into mere paperwork drills. Department of Defense agencies have faced years of congressional oversight, forcing development of acquisition and security management practices and programs. Many non-DOD agencies do not have fully implemented information security programs in place that would include the conduct of comprehensive risk or vulnerability assessments.

The Y2K drill forced many non-DOD agencies to take a number of planning and remediation actions that were outside of their normal operating procedures. The effect of heightened congressional oversight, popularized by the grading system[7] brought tremendous management pressure on agency information security officials. This has been perpetuated by the new round of scoring on computer security postures of federal agencies prepared by Representative Stephen Horn (R-CA), chairman House Government Management, Information and Technology Subcommittee.[8]

---

[6] Press Briefing on the Report of the Accountability Review Boards on the Embassy Bombings in Nairobi and Dar Es Salaam, January 8, 1999 Washington, D.C. Comments from Admiral William J. Crowe, Chairman URL: http://www.state.gov/www/policy_remarks/1999/990108_emb_rpt.html

[7] Tillett, Scott L, Feds receive 'above average' grade on Y2K, Federal Computer Week, 11/22/1999 URL: http://www.fcw.com/fcw/articles/1999/fcw_11221999_horn.asp

[8] Subcommittee on Government Management, Information and Technology, Committee on Government Reform,

The cumulative effects of these reports, directives and congressional oversight are clearly reflected in the Department of State. There has been a dramatic improvement in the security posture of the Department of State over the last two years. The Department of State has developed new programs to address assessing risk, increased controls, monitoring and evaluation, and increased security awareness training. The Department of State was among the top four federal agencies in the first round of grading by the Horn subcommittee, rating a "C"[9], after receiving a scathing report from the General Accounting Office in March 1998.[10]

The increase in attention to information security issues within the Department of State has resulted in information security programs receiving more support and understanding from management. This has increased program effectiveness and enhanced the ability of security programs to improve the overall level of protection to the Department's systems.

The Department of State is in the planning stage to allow Internet access to the desktop, part of a series of recommendations from the Stimson Report[11] and the Overseas Presence Advisory Panel.[12] This will introduce new vulnerabilities to the Department of State, which are being reviewed prior to implementation of the pilot. The vulnerability assessments conducted in development of the pilot will support future risk management decisions regarding introducing Internet access to the Department's system.

Traditionally when agencies conducted risk assessments or analyses of their systems they were conducted with a computer-centric perspective. The conduct of a, PDD 63 relevant, vulnerability assessment requires a different perspective. No longer is it sufficient to see if building access controls are in place, now the assessor has to address the potential for those access controls to be by-passed and what risk that might represent to a critical or essential resource (often a network system). The resulting analysis leads to the identification of threat pathways that must be reviewed for credibility. The process of determining credible threats is an iterative process involving the assessor and resource owners. Once a credible attack scenario has been validated (i.e., the resource owners agree that the threat pathway is valid), a table top exercise is conducted with vulnerability assessment team members, resource owners and other agency subject matter experts as warranted. These exercises result in scoring the likelihood that the attack scenario would impact the target to an unacceptable level.

The conduct of vulnerability assessments, along the PDD 63 model, will provide senior managers a broader view of the environment in which the agency or business operates, the internal and external forces that can effect the system and the limits that face the organization in

---

First Report Card on Computer Security at Federal Departments and Agencies, September 11,2000 URL: http://www.hours.gov/reform/gmit/hearings/2000hearings/000911co…/00091reportcard.htm

[9] Ibid.

[10] Computer Security: Pervasive, Serious Weaknesses are Putting State Department Operations at Risk (GAO/C-AIMD 98-47) March 1998

[11] Stimson Center, Managing U. S. Foreign Affairs in the 21st Century October 1998, URL: http://www.stimson.org/oop

[12] U. S. Department of State, The Report of the Overseas Presence Advisory Panel, November 1999 URL: http://www.state.gov/www/publications/9911_opap/rpt_99111_opap.pdf

controlling or mitigating potential threats. The conduct of risk assessments, or more effectively vulnerability assessments provides the initial base to support risk management decisions in any organization.