# Global Information Assurance Certification Paper

**Jerry L.Davis**

# IMPLEMENTATION OF TECHNICAL ELEMENTS I, II, AND III OF THE CRITICAL INFRASTRUCTER PROTECTION PLAN:

## *THE ROLE OF THE INFORMATION ASSURANCE PROFESSIONAL*

### Scope:

This paper will first define and discuss the Critical Infrastructure Protection Plan. Within this discussion, the first three elements that compose the Critical Infrastructure Protection Plan will be delineated. Along with this delineation, instruction will take place to show what steps the Information Assurance Professional (IAP) can follow to help institute those first three elements. The instruction provided includes an overview of methodologies that can be used; identification of cyber based threat and vulnerability information repositories, and how the use of these tools will help to construct the first three elements of the Critical Infrastructure Protection Plan.

### Discussion:

Presidential Decision Directive 63 (PDD-63) of May 1998 [1], sets forth the criteria for the national effort to be undertaken that will ensure that those federal agencies and their critical cyber and non cyber based infrastructures that compose the United State's critical infrastructure be protected. To comply with PDD-63, federal agencies must develop and institute a robust and comprehensive 12-element plan that describes largely how they will identify and protect critical assets. This 12-element plan is known as the Critical Infrastructure Protection Plan (CIPP) and ensures to some larger degree that there will be continuity of the federal government in the event of some catastrophic event. It is assumed that this catastrophic event, if carried out, may have a significant and lethal impact on our nation as a whole. These 12 elements as defined by the Critical Infrastructure Assurance Office (CIAO), are broken into two sections, Technical and Management and Administration. They are as follows:

**Technical**

1. Agency Mission and Identification of Mission-Critical Infrastructure.
2. Threat Analysis
3. Vulnerability Assessment
4. Remedial Plans
5. Emergency Plans
6. Research and Development Needs

**Management & Administrative**

7. Roles & Responsibilities
8. Resource Requirements
9. Coordination Efforts
10. Recruitment, Retention, Education & Awareness Efforts



© SANS Institute 2000 - 2005 Author retains full rights.

11. Implementation Schedule/Revised CIPP
12. Authorities & Guidance

Though all of these elements are necessary implementations to devising a formidable CIPP, the first three of these elements are the most crucial to the understanding of the IAP when set forth to design plans that will first identify and then assess threats and vulnerabilities to critical information systems. The IAP ensures that those critical information systems (considered to be a critical infrastructure asset), once identified, are protected against those threats that are common to information systems. Furthermore, the IAP must discover and make recommendations to mitigate those vulnerabilities that are unique to the information system under assessment.

*Element I- Identification of Critical Missions & Mission-Critical Infrastructure Assets.*

What exactly are those mission critical information systems? Well to properly identify those systems within an agency, that agency, office, division, or component must have been designated as having a *critical mission*. Still, however, the question must remain; how does one go about defining what missions are critical to an agency? For an agency to be designated as having a critical mission, some predetermined *criteria* must be in place so that the mission can first be defined and then leveraged against those standards of criteria to be designated as critical. Once the mission is recognized as critical, then the agency can be included as being a part of the nation's critical infrastructure. There subsist with in the federal government domain a number of criterions that can be used to ascertain if an agency's mission is critical.

One of these domains is the CIAO. The CIAO is first acknowledged in PDD-63 and it's purpose is to serve as the an oversight and implementation support vehicle for PDD-63 [2] by creating alliances between government and private sector entities to formulate a national plan. This alliance was to devise and pin point critical infrastructure elements and to jointly formulate a plan that would help protect those elements. The logic behind this marriage came about during the summation of a government review that studied and documented the nation's critical infrastructure elements. The results of this study proved that most national critical infrastructure elements originated largely from, and belonged to, private sector entities.

Upon review of the CIAO, we see several rudiments of criterion which are used to establish the criticality of a particular agency. Some of these criterions are mentioned in brief format under the Project Matrix Overview. Project Matrix was conceived from within the CIAO and proposed the groundwork that would be the standard and template model for all federal sector agencies to emulate when implementation of PDD-63 was initiated [3]. Project Matrix in its model defines ***critical*** as:

**Responsibilities, nodes, and networks, which if incapacitated or destroyed would:**

- Jeopardize the nation's survival.
- Have a serious, deleterious effect on the nation at large.
- Adversely affect large portions of the nation's populace
- Require near term, if not immediate, remediation.

The above listed criterions are primarily guidelines in helping to accurately establish those agencies that are included a part of the critical infrastructure inside the US. In the CIAO, these critical infrastructures are defined as Mission Essential Infrastructure (MEI). However, just because a particular agency's mission does not meet all the criteria set forth as critical within the Federal Government, does not at all mean that it's existence or lack thereof is not critical in part to it's *stakeholders*. Therefore, other criterions can and should be developed internally by the agency under assessment so that the agency's mission under review can be leveraged against those criterions to determine criticality locally (i.e. within the agency and to the stakeholders). Stakeholders are those individuals (i.e. the end beneficiary), who vehemently rely upon and benefit from the services provided by the agency in question. Therefore, the lost or severe impediment of those services to the stakeholder will cause a serious and aggravating negative impact to the said stakeholder. So only by careful review of the mission, leveraged against some predetermine national and internal criterions, can it be established that the mission is in fact critical.

Identification of Critical Agencies Process:

**Feeder Information:**

- **Review of determining criteria for critical status**
- **Review of Agency's mission**
- **Mission leveraged against criteria**

**Extracted results:**

- **Defined critical agency and mission**

Now that the critical agencies and their respective critical missions are identified, the IAP must engage in a comprehensive review of those information systems that support the agency's critical mission. This is done through documentation review relevant to those information systems, interviews with key personnel relevant to the information systems and by fostering a trusting relationship with the client to gain as much knowledge about the information systems as possible. Once these tasks are completed and the IAP has an in-dept understanding of the information system under review, then the criticality of the information flowing through an information system can be determined. Care and consideration should be taken into account when conducting this phase of the task. Adequate time should be allowed for a thorough review of as much documentation and to allow as many interviews as possible.

The questions that drive the determination of whether an information system can be

defined as critical should be derived from the criterion established earlier. At a minimum, the IAP should always bare in mind what the impact to the stakeholder would be should the service provided by the information system become unavailable or seriously impeded. How one goes about determining which persons to interview, what questions to ask, and what documents to review, does not have to be re-invented. The CIAO has endorsed two well know processes for conducting information assurance assessments for information systems as well as physical security vulnerability assessments [4]. Those agencies/methodologies are:

- The National Security Agency's (NSA) Information Security Assessment Methodology (IAM)
- The Defense Threat Reduction Agency (DTRA) Critical Infrastructure Vulnerability Assessment (CIVA) course.

Both of these agency's methodologies have proven to be effective and well received. In fact, the NSA methodology comes by way of a partnership with the National Institute of Standards and Technology [5]. This partnership known as the National Information Assurance Partnership (NIAP) and is beneficial in that it allows private sector consultants to attend the IAM course and become certified in implementing the IAM industry wide. Likewise, DTRA's CIVA methodology course provides a plethora of information and guidance on installation vulnerability assessment methodology, team composition and assessment activity.

Identification of Critical Information Systems Process:

**Feeder Information:**

- **Application of a CIAO endorsed methodology**
- **Document review**
- **Interviews of relevant personnel**

**Extracted results:**

- **Critical information systems identified**

*Element II-Threat Analysis*

A threat can be defined as**: *Any indication, circumstance or event with the potential to cause damage or loss of or damage to an asset*** [6]**.**

Now then, the critical systems are identified so what are the threats to these systems, or rather how does the IAP determine what the threats are? This is where research, experience, expertise, and common sense (of which a good mentor of mine once told me that this trait is rarer than money) comes into play. Threats to an information system that are normally identified for the purpose of establishing a security plan, comes in several flavors [7]. Some of these flavors are:

- Malicious
- Natural
- Accidental
- Intentional
- Non-malicious

Some of these threats can further be broken down as having origins that are from either internal or external sources. We know (or rather should know) from our vast knowledge of infinite wisdom and our large database of "gee whiz" sources of information and statistics that our threat profile includes but is not limited to the following threat profiles.

| Threat | Malicious | Accidental | Intentional | Non-Malicious | Natural |
|---|---|---|---|---|---|
| Hacker crackers | X | | X | | |
| Viruses | X | | X | | |
| Trojan Horses | X | | X | | |
| Worms | X | | X | | |
| Typical Employee | | X | | X | |
| Disgruntled employees | X | | X | | |
| Earthquakes | | | | | X |
| Floods | | X | | | X |
| Power outages | | X | | | X |

Once the IAP has defined the threats to the information system, analysis of these threats must be concluded. When the threat is analyzed, the IAP must understand some common threat characteristics. Normally one threat is a combination of two or more threats rolled into one and then launched against a target. Hence, the purpose (intention) for which the threat is in-acted may not be readily apparent. In other words, it may be true that a virus is in fact written and introduced for the sole purpose to *intentionally* cause some sort of *malicious* havoc on whatever network or system it is introduced into. But the fact that the unwitting employee (also read, threat non-malicious type) who released the virus onto the system by failure to scan a floppy disk is an *unintentional*, and perhaps even an *accidental* co-conspirator to rendering the system useless. So, here one can see how two different threats, one with intentions of complete malice, and another threat with no harmful intentions whatsoever, can interact to produce potentially negative results.

The IAP should have a strong arsenal of threat databases from which to gather threat

information. Several very helpful and unique publicly available accredited cyber based repositories of threat information exists for this very reason. At the very least the IAP should consult:

- The National Infrastructure Protection Center (NIPC)
- The Federal Computer Incident Response Center (FedCIRC)
- The Carnegie-Mellon University (CMU) Computer Emergency Response Team (CERT)
- The Security Administration, Network and Security (SANS) Institute

NIPC is another institution that was driven out of the requirements set forth in PDD-63 [8], and is based in the Federal Bureau of Investigation's headquarters facility. The NIPC provides an excellent indication and warning capability for those who tap into it.

Another valuable resource is FedCIRC. Also driven by requirements of PDD-63, FedCIRC is a sort of one stop shop for incident reporting, handling, prevention and recognition. FedCIRC uses the supporting information contained within the reporting data of cyber based related security topics from both security and law enforcement [9] organizations.

Perhaps one of the most well known and used repositories for collecting threat data is the CERT at CMU. The CERT was established in 1988 by the Defense Advanced Research Projects Agency (DARPA now ARPA) after the malicious code Morris Worm incapacitated some 10% of all computers connected to the Internet. The CERT is capable of providing support in number of computer security areas. The CERT Coordination Center (CERT/CC) provides endless volumes of pertinent information on Internet security vulnerabilities. In addition, they provide incident response services to casualties of Internet attacks, provide development on information and training, and publish a number of security alerts [10].

The SANS Institute is a core community of nearly 100,000 systems administrators, security personnel, and network administrators who provide input, guidance, expertise, and years of experience in research to share their lessons learned and find solutions to security vulnerabilities. SANS also distributes a number of security alerts, news updates and publications. Like the CERT, SANS is one of the most well known respected, and used repositories for the collection and dissemination of security related information on a global scale [11].

One last final item that is more often missed when the threat data base is constructed is that threat that the client has concerns over. Often, the IAP can be narrow in scope when resolving threat issues that are commonly known to information systems. However, those concerns or threats that are the perception of the client must be taken under review also. A well-rounded IAP knows the various threats, categories of threats, maintains a threat database, or at least knows where to find the correct

information on threats. Often though, the client has other threats in mind outside those commonly known threats that is undoubtedly unique to the institution they govern. With that understanding, it is the duty of the IAP to ensure that that they investigate this issue and include the findings in the threat database.

Threat Analysis Process:

**Feeder information:**

- **Identification of the critical missions**
- **Identification of the critical infrastructure assets (critical information systems)**
- **Query of threat databases and repositories (SANS, NIPC, etc.)**
- **Apply knowledge of existing threats (Human, malicious code, etc.)**
- **Client's perception of threat (those unique to the client's environment)**

**Extracted results:**

- **Properly identified threats to the critical information system**

Element III-Vulnerability Assessment

Vulnerability can be described as: ***Any weakness that can be exploited by an adversary to gain access to an asset*** [12]**.**

Vulnerability assessments will cause most IAPs to perk up immediately just upon hearing the term. The heart probably beats a little faster and the adrenaline levels probably rises pretty rapidly. Thoughts of running ISS tools, Cyber Cop, Nmap, Neo Trace, war dialers, and putting together a good social engineering plan comes to mind almost instantaneously. Unfortunately, it's not *that* type of vulnerability assessment. Likewise it is also **not** a penetration test! Vulnerability assessments conducted on behalf of constructing CIPPs are *non-intrusive* (note the operative word non.). It is primarily conducted through the use of interviews, documentation review, and system demonstrations. Not to be forgotten, prior knowledge, expertise, experience, and the ever so elusive common sense, on the part of the IAP should also be tapped into.

To perform a good vulnerability assessment, those threats identified earlier need to be leveraged against a perceived or known vulnerability in addition to the assessment being undertaken. Security policy review, systems demonstrations, network architecture and topology reviews, continuity of operations plans, disaster plans and personnel interviews at various levels are the just some of subjects that give the IAP a framework as to what the vulnerabilities are once they are leveraged against those defined threats.

IAPs need to ask themselves questions upon reviewing documents like the network architecture such as: "Are the firewalls configured properly according to the security policy?" " Are logs system logs audited regularly?" Similarly when performing task

such as system demonstrations IAPs may want to ask questions like: "Do users scan disk from an unknown source before accessing the contents?" "Are screen saver passwords used?" "Are passwords located on sticky notes posted on the monitor?" (Or under the keyboard, bottom of desk drawers, or in some cases, on the ceiling over the user's head). Other items may include if updated patches are applied, whether or not virus definitions are current, etc., etc., etc.

After the IAP has reviewed all the proper documents, interviewed key personnel, and participated in system demonstrations, he/she may then begin to put together a final report on findings and recommendations. The findings are those vulnerabilities that were found to exist on the information system assessed. The final report generated should reflect the identification of those critical information systems, the threats to those systems, and the vulnerabilities found after the assessment portion was conducted. The report should further include recommendations that would mitigate those vulnerabilities found. Recommendations should include, but is by no way limited to items such as the installation of patches, firewall configuration, the use of routers, the use of intrusion detection systems, physical security items, anti-virus signature updates, and most important than all, **security training and awareness!**

## Vulnerability Assessment Process:

**Feeder Information:**

- **Consultation of the threat database**
- **Application of best practices, expertise and experience**
- **Documentation review**
- **Interviews of key personnel**
- **System demonstration observations**

**Extracted Information:**

- **A completed vulnerability assessment plan**
- **A final threat and vulnerabilities assessment plan with proposed recommendations**

## CONCLUSIONS

The proper institution of the initial three elements of Critical Infrastructure Protection Plan can be a tedious and challenging task for the Information Assurance Professional. Depending on the size of the institution needing the plan, there may be tens to hundreds of critical information systems needing identification, hundreds of interviews to be conducted and likewise hundreds of vulnerabilities to be defined. A solid and viable Critical Infrastructure Protection Plan is one that will ensure to some extent that critical information systems operated within an agency can withstand cyber as well as non-cyber attacks of different varieties and intensity while continuing to provide it's critical services to

the intended stakeholders.

The steps by which this process is enacted begins with first defining the critical missions of the agency under assessment based on some predetermined national and internal agency criteria. Once those critical missions are defined, critical assets, which include information systems that are critical to the implementation of those missions must be identified. Next, through the use of common knowledge, expertise, experience, and consultation of threat repositories the threat to those should be reviewed. Finally, vulnerabilities organic to information systems can be defined and recorded through the use of key personnel interviews, documentation review, system demonstrations, application of expertise, experience and best practices used. The conglomeration of all this information should lead the IAP into creating a very well defined findings and recommendation proposal that mitigates the pejorative effects of those vulnerabilities identified.

## REFERENCES


1. The White House, *Presidential Decision Directive/NSC-63*, May 22, 1998. http://209.207.236.112/irp/ofdocs/pdd/pdd-63.htm

2. The White House Office of the Press Secretary, *Protecting America's Critical Infrastructure: PDD 63,* May 22, 1998. http://www.ciao.gov/press_release/WhiteHouseFactSheet_PDD63.htm

3. Clarke, Richards. *Implementation of PDD-63 through Project Matrix*. Memorandum Critical Infrastructure Assurance Office, July 19, 2000. http://www.ciao.gov/Matrix/RC_Memo.htm

4. The National Information Assurance Partnership, *InFosec Assessments Abstract*. http://niap.nist.gov/niap/projects/infosec-proj.html (November 2, 2000)

5. The White House, *National Plan for Information Systems Protection*. Version 1. 2000 http://www.ciao.gov/National_Plan/national_plan_final.pdf (November 2, 2000)

6. Central Intelligence Agency Office of Facilities and Security Services, Analysis Brach, *Analytical Risk Management, A Systems Approach to Security Decision-Making,* September 25, 1995. Pg. 20

7. The White House, *National Plan for Information Systems Protection*. Version 1. 2000, pg. 45 http://www.ciao.gov/National_Plan/national_plan_final.pdf (November 4, 2000)

8. The White House, *National Plan for Information Systems Protection*. Version 1. 2000, pg. 25 http://www.ciao.gov/National_Plan/national_plan_final.pdf (November 4, 2000)

9. US Government, The Federal Computer Incident Response Capability, about FedCIRC. http://www.fedcirc.gov/ (November 9, 2000)

10. Mellon, Carnegie, The Computer Emergency Response Team, Coordination Center, home page. http://www.cert.org/index.html (November, 10, 2000)

11. The System Administration, Network and Security Institute, about us page, http://www.sans.org/aboutsans.htm (November 10, 2000)

12. Central Intelligence Agency Office of Facilities and Security Services, Analysis Brach, *Analytical Risk Management, A Systems Approach to Security Decision-Making,* September 25, 1995. Pg. 30