RECOMMENDATIONS FOR A STANDARDIZED PROGRAM MANAGEMENT OFFICE (PMO) TIME COMPLIANCE NETWORK ORDER (TCNO) PATCHING PROCESS

THESIS

Michael Czumak III, 1 LT, USAF

AFIT/GIR/ENV/07-M8

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/07-M8

RECOMMENDATIONS FOR A STANDARDIZED PROGRAM MANAGEMENT OFFICE (PMO) TIME COMPLIANCE NETWORK ORDER (TCNO) PATCHING PROCESS

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Michael Czumak III, BA

Lieutenant, USAF

March 2007

AFIT/GIR/ENV/07-M8

RECOMMENDATIONS FOR A STANDARDIZED PROGRAM MANAGEMENT OFFICE (PMO) TIME COMPLIANCE NETWORK ORDER (TCNO) PATCHING PROCESS

Michael Czumak III, BA

Lieutenant, USAF

Approved:

/signed/	22 February, 2007
Michael R. Grimaila, PhD (Chairman)	Date
/signed/	22 February, 2007
Alan R. Heminger, PhD (Member)	Date
/signed/	22 February, 2007
Maj David Kaziska, PhD (Member)	Date

Abstract

Network security is a paramount concern for organizations utilizing computer technology, and the Air Force is no exception. Network software vulnerability patching is a critical determinant of network security. The Air Force deploys these patches as Time Compliance Network Orders (TCNOs), which together with associated processes and enforced timelines ensure network compliance. While the majority of the network assets affected by this process are Air Force owned and operated, a large number are maintained by external entities known as Program Management Offices (PMOs). Although these externally controlled systems provide a service to the Air Force and reside on its network, the TCNO processes for these assets are dictated and managed, to a large extent, by the PMOs. There is no current or planned, standardized method to release TCNOs to PMOs within the AF. Some are notified and tracked through a portal by the AFNOSC, while others are notified and tracked via secure email by MAJCOM NOSCs. While AFI mandates that PMOs are responsible for establishing procedures to evaluate applicability to their systems, there are no quality checks, standardization requirements or oversight to ensure the results of such evaluations are sound. Nonetheless, these PMO systems directly impact the security of the Air Force Network and the Department of Defense at large. By examining existing PMO patch management processes, this study should provide a better understanding of the TCNO processes used by PMOs with the intent of exploiting strengths and addressing weaknesses in an effort to move towards a standardized TCNO patching process.

To my loving wife

Acknowledgments

I would like to thank my research advisor, Dr. Grimaila, whose willingness to lend support and expertise regardless of time or day, allowed me to complete this effort successfully. I also wish to thank my committee members, Dr. Heminger and Maj. Kaziska. Their insight and efforts directly contributed to a more rigorous methodology and a properly executed research process.

I would also like to thank the participants of this research study. Although I cannot name them individually, their involvement requires additional mentioning, for without their honest contributions, this research would not have been possible. In addition, I would also like to extend thanks to my research sponsor, Air Force Network Operations Center, Detachment 1, Eighth Air Force, who provided me with the necessary information and contacts to make this research effort a success.

The steadfast friends that made up my support structure here at AFIT (you know who you are) had a direct impact on my success and I thank you. Finally, this effort would not have been possible without the unwavering support of my loving wife, whose selflessness and understanding allowed me to complete this work successfully.

Michael Czumak III

Table of Contents

Page

Abstract iv
Acknowledgments vi
Table of Contents vii
List of Figures x
List of Tables xi
I. Introduction 1
Background 3
Problem Statement 5
Research Objectives/Questions/Hypotheses 6
Assumptions/Limitations 7
Benefits/Implications 8
II. Literature Review 10
Chapter Overview 10
Air Force Instruction 10
MAJCOM Guidance 19
Pending Guidance 19
Accepted Patch Management practices 20
Summary 31
III. Methodology 32
Chapter Overview 32
Type of design 32
A study's questions 33

Page

Study propositions 35
Unit(s) of analysis 36
Data collection strategies 37
Data analysis strategies 42
Methods of achieving validity 43
Overview of the Interview Process 46
Summary 46
IV. Analysis and Results 47
Overview 47
Initial Data Collection and Analysis 47
Site Selection 53
Interviewee Participants 54
Results 55
V. Conclusions and Recommendations 67
Overview 67
Answers to Research Questions 67
Answers to Propositions 76
Limitations 78
Recommendations for Future Research 78
Conclusion 80

Page

Appendix A: Case Study Protocol and Case Study Database Format 81
Appendix B: Selection Criteria Data 114
Appendix C: Human Subjects Exemption Approval 119
References 120

List of Figures

Page

Figure 1: Security Vulnerabilities Reported 1995-2006 3

Figure 2: Air Force TCNO notification and tracking hierarchy 11

Figure 3: Apparent TCNO distribution process 70

List of Tables

Page

Table 1: Air Force TCNO priority categories 15

Table 2: Air Force TCNO suspense dates 16

Table 3: Air Force TCNO extension approval process 18

Table 4: PMO Site Selection and Performance Data 53

Table 5: PMO Site Selection and Performance Data 53

Table 6: PMO Interviewee Information 54

Table 7: TCNO Distribution 56

Table 8: TCNO Acknowledgment 58

Table 9: TCNO Applicability Assessment 58

Table 10: TCNO Testing 59

Table 11: TCNO Installation 61

Table 12: TCNO Reporting 63

Table 13: TCNO-D Status Levels 63

RECOMMENDATIONS FOR A STANDARDIZED PROGRAM MANAGEMENT OFFICE (PMO) TIME COMPLIANCE NETWORK ORDER (TCNO) PATCHING PROCESS

I. Introduction

Network security is a paramount concern for organizations utilizing computer technology, and the Air Force is no exception. In a ten year timeframe, the number of reported security vulnerabilities has risen from 100 in 1995 to almost 6000 in 2005 (see Chart 1) (CERT, 2006). In addition, the director of CERT, Carnegie Mellon's center of Internet security expertise, estimated as much as 80 percent of security incidents go unreported due to lack of knowledge or organizational reluctance to report (GAO, 2003, 8). It is clear that security incidents prove costly to all organizations worldwide. In 2004, a Congressional Research Service study estimated that major virus attacks alone cost $12.5 billion (Congressional Research Service, 2004). This is just a portion of the estimated $470 billion to $580 billion of worldwide economic damage caused by digital attacks in 2005 (Wall, 2006). In response to these costly threats organizations have implemented safeguards to intercept attacks and eliminate vulnerabilities. U.S. companies alone are expected to spend $10 billion in 2006 on security compliance (Wall, 2006).

Network software vulnerability patching is one accepted method of mitigating these vulnerabilities and as such is a critical determinant of network security. In fact,

according to CERT, “about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches” (GAO, 2004, 6). The process used to govern the implementation of these network vulnerability patches is commonly referred to as patch management (GAO, 2003, 11). Although individual steps of the patch management process sometimes vary slightly among organizations, the overall process follows a common progression from acquisition to application of the patch.

The Air Force deploys network security patches as Time Compliance Network Orders (TCNOs), which together with associated processes and enforced timelines ensure network compliance. While the majority of the network assets affected by this process are Air Force owned and operated, a large number are maintained by external entities known as Program Management Offices (PMOs). According to Air Force Instruction 22-138, a PMO *develops, acquires, and fields technical solutions for Air Force-networks and systems* and *exist at the Air Force and MAJCOM levels* (AFI33-138, 2005). Although these externally controlled systems provide a service to the Air Force and reside on its network, the TCNO testing and installation processes for these assets are dictated and managed, to a large extent, by the PMOs. Because there are a large number of PMOs, each with their own testing and implementation procedures, TCNO compliance amongst these machines often exceeds the mandated Air Force time frame. As a result, PMO asset security and subsequently the security of the Air Force Network, is degraded.

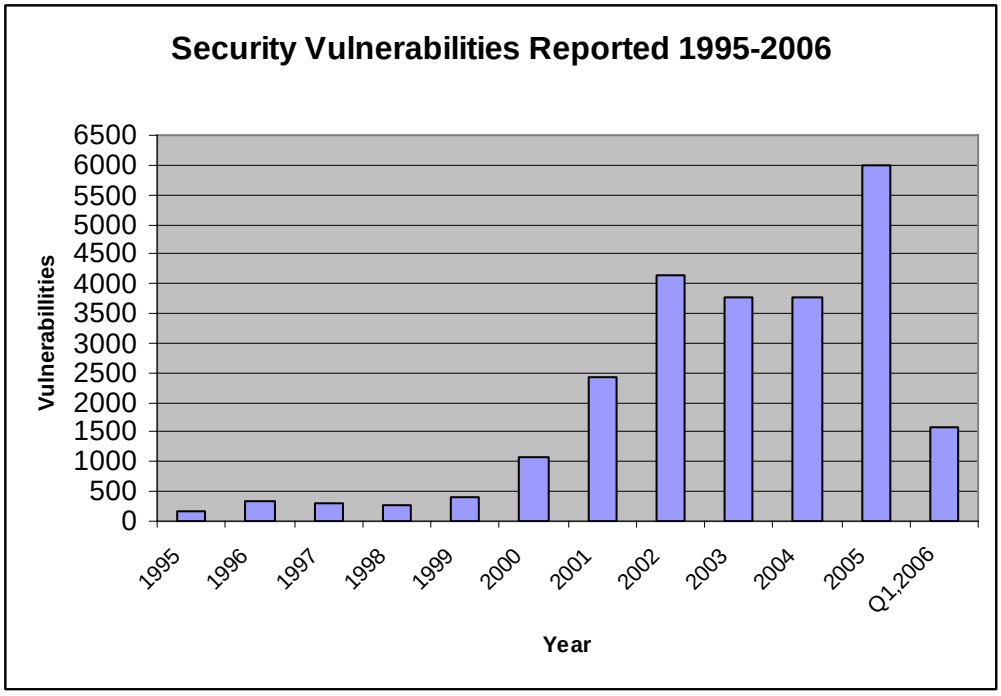


Figure 1: Security Vulnerabilities Reported 1995-2006 (CERT 2006)

Background

In 2003, the Air Force Chief Information Officer expressed an organizational goal of reducing TCNO deployment time to twenty-four hours, from initial release to patch installation (Gilligan, 2003). This direction, coupled with the increasing awareness that TCNO installation is both a necessary and growing function has spurred numerous process improvement initiatives. When security patching was in its infancy, network patches were installed manually, which was a labor intensive and unrelenting process. With the introduction of centrally managed, electronic installation methods, many of today's TCNOs are installed remotely on a large scale. However, because PMO assets are unique in the software applications they run, TCNOs must be extensively tested prior

to installation on these machines. As a result, remote installation is not an option and in most cases prohibited by Air Force instruction (AFI33-138, 2005). Instead, the PMO office responsible for the system to receive the TCNO must first determine applicability of the patch, and if it is deemed appropriate, test the patch prior to allowing installation on its machines. This testing and installation process is not overseen by the Air Force and as a result, time frames of TCNO installation amongst PMOs can vary considerably.

The current AF method to track and manage the TCNO process amongst its many PMOs is extremely limited and fragmented at best. According to the AFNOSC, there is currently "no way of tracking or verifying what individual PMOs do for testing TCNO applicability" (Matthews, 2006). New, upcoming systems are anticipated to provide the capability for remote "remediation" or application of the TCNO, without the need for excessive coordination through MAJCOMs and base-level entities. However, "most if not all PMO systems will be put into an "exceptions" list for remediation" (AFNOSC, 2006), and therefore will not benefit from such process improvements. The AF uses a tool called the TCNO Dashboard to track PMO TCNO compliance. When using this tool, PMOs must register their TCNO assessment/testing program for review and acknowledge and update their status for each TCNO that is released by the AFNOSC. However, at this time "less than 10% of PMO are registered within the TCNO Dashboard" (AFNOSC, 2006) and there is no policy mandating them to do so. Additionally, since this is an AFNOSC tool meant for AF level-PMOs, it only tracks a portion of the total PMOs on the Air Force network.

Problem Statement

There is no current or planned, standardized method to release TCNOs to PMOs within the AF. Some are notified and tracked through a portal by the AFNOSC, while others are notified and tracked via secure email by MAJCOM NOSCs. While AFI mandates that PMOs are responsible for establishing procedures to evaluate applicability to their systems, there are no quality checks, standardization requirements or oversight to ensure the results of such evaluations are sound. Nonetheless, these PMO systems directly impact the security of the Air Force Network and the Department of Defense at large.

Previous thesis research has examined the Air Force TCNO creation and implementation process in an effort to identify shortfalls and offer suggestions for improvement and further research (Kubinsky, 2004). One of the identified problems in this thesis was the lack of a standardized process governing TCNO disbursement to PMOs. Also identified was an unnatural order of events for TCNO distribution events which prevents the PMO offices from receiving TCNOs in a timely manner. However, the research did not examine in any detail individual PMO testing and implementation or distribution procedures for TCNOs and as a result recommended this as a future research consideration. A request for further research has come from the AFNOSC, which is currently putting together a plan to improve the Air Force's TCNO process and has yet to look into the PMO issue in great detail.

Research Objectives/Questions/Hypotheses

In order to improve existing PMO patch management methods, we must examine the entire process including patch distribution, assessment, testing, patching and reporting practices used by PMOs operating within the bounds of the Air Force network.

Air Force instruction 33-138 states "the goal of the TCNO process is the mitigation of risk to the AFEN through the implementation of network vulnerability countermeasures" (AFI 33-138, 3.16) and "achieving 100% compliance with all TCNOs is and will remain the ultimate goal to ensure the security and integrity of the AFEN and the information contained therein" (AFI 33-138, 3.31). It goes on to state that "the timely up-channel flow of TCNO compliance statistics through the AFNETOPS hierarchy provides a picture of overall risk to the AFEN and Air Force information systems" (AFI 33-138, 3.28), establishing a direct relationship between timely TCNO deployment and network security. Consequently, this study will examine whether the lack of standardized, centrally managed, and enforced security patching procedures for Air Force PMO assets leads to lateness of network system TCNO compliance and in turn, weakens the security of the Air Force Network by addressing the following questions:

RQ1). How does the lack of standardized, centrally managed, and enforced TCNO patching procedures for PMO impact the TCNO compliance timeframe and in turn, the security posture of the Air Force Network?

SRQ1). How do the methods of TCNO distribution (both to and from the PMOs) impact the TCNO compliance timeframe?

SRQ2). How do PMO applicability assessment methods impact the TCNO compliance timeframe?

SRQ3). How do PMO testing methods impact the TCNO compliance timeframe?

SRQ4). How do PMO patching methods impact the TCNO compliance timeframe?

SRQ5). How do PMO reporting methods impact the TCNO compliance timeframe?

SRQ6). Are there any additional organizational behavior issues that might impact the TCNO compliance timeframe?

Assumptions/Limitations

Patch management and the implementation of security patches is just one of numerous security management practices that are necessary for maintaining appropriate levels of network security. Other methods including firewalls, user education, passwords

etc., while important, are beyond the scope of this research and will therefore only be addressed as reference points as deemed necessary by the author. Furthermore, the argument for or against the use of patch management as an effective security practice will not be considered. Since it is a widely accepted practice across industries and organizations including the Air Force, the need for a patch management process is assumed for the purposes of this study.

The process of patch management spans the entire Air Force organization. While focusing solely on PMO patch management narrows the focus considerably, it is still unfeasible to consider studying all PMOs and associated processes in the time frame allotted for this study. Therefore, some decisions will be made as to which PMOs and Air Force organizations will be studied within the context of this problem. Additionally, while there are numerous steps in the patch management process, this study will not address the processes of initially identifying network vulnerabilities or creating the initial TCNO. Instead, it will begin at the point of distribution and follow the TCNO through the PMO evaluation, testing and installation processes. The Air Force TCNO installation process will be examined on a limited basis only for the purpose of comparing TCNO compliance rates with those of PMOs.

Benefits/Implications

Information systems are only as good as the security patches that have been applied (Qualls, 2004). "It only takes one missed or improper patched system to jeopardize the whole computing environment in an organization" (Chan, 2003). Without a standardized process to ensure patching is completed in a timely manner, the Air Force

runs the risk of compromising the security of it network and the mission-critical information contained within. To illustrate this security risk, TCNO compliance data collected over a five year period shows that PMO assets accounted for over 189,000 security vulnerabilities on the Air Force Network (Action Tracker historical data, 2001-2006). As a result, PMO systems that reside on the AF Network must be governed by such a process to ensure their compliance with Air Force security standards. By examining existing PMO patch management processes, this study should provide a better understanding of the processes used by PMOs to determine applicability, test, and implement Air Force directed TCNOs and how those processes fit into the overall AF TCNO management process with the intent of identifying any weaknesses in the current processes and offer recommendations to the Air Force as to how to address such weaknesses.

II. Literature Review

Chapter Overview

The purpose of this chapter is to expand upon the information presented in Chapter 1 through relevant literature. First, applicable regulations that govern the Air Force TCNO process will be addressed to provide a basic understanding of the regulations that Air Force organizations and PMOs must adhere to when conducting patch management. Following, the major steps of a successful patch management program will be examined by presenting professional literature to provide a thorough understanding of the process and introduce some commonly used "best practices" among various organizations.

Air Force Instruction

Agencies and their responsibilities

The Air Force TCNO process is governed by Air Force Instruction (AFI) 33-138. This instruction outlines the roles and responsibilities of all applicable organizational units interfacing with the Air Force network. A hierarchal representation appears in Figure 2. For the purposes of this study, the process is limited to the AFNOSC and all organizations within its purview, so the discussion of the responsibilities of JTF-GNO will be limited. Also, a System Program Office (SPO) has the same function of a PMO, but usually comes under the administrative authority of Air Force Material Command or Air Force Space Command. For the purposes of this study SPOs and PMOs will be treated identically and will be addressed universally as PMOs.

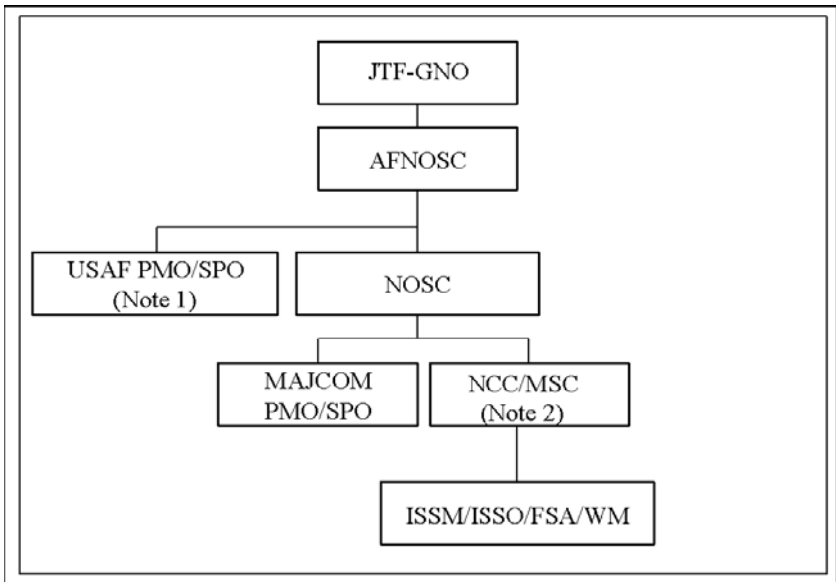


Figure 2: Air Force TCNO notification and tracking hierarchy (AFI 33-138, 2005)

JTF-GNO

The responsibilities of JTF-GNO (USSTRATCOM) are outlined in Chairmen of the Joint Chiefs of Staff Notice (CJCSN) 6510.01 CH 2, January 26, 2006. JTF-GNO releases network vulnerability patches in the form of IAVAs, which are provided to the various Department of Defense (DoD) components for compliance. The Air Force, being one such component, tracks these IAVAs as TCNOs through the AFNOSC. JTF-GNO monitors IAVA compliance and asset status across the DoD. While understanding this relationship helps to see how the Air Force obtains some of its vulnerability patches, not all TCNOs are generated from DoD IAVAs. Some TCNOs are generated by the AFNOSC and Air Force MAJCOMs in response to a perceived threat internal to the Air Force network and have no reporting relationship with JTF-GNO. Additionally, the

policies and procedures associated with Air Force PMO compliance are not dictated by JTF-GNO, so their influence on the process of interest to this study is minimal.

AFNOSC

According to AFI33-138, the AFNOSC serves as the Air Force office of primary responsibility to generate, disseminate, and track implementation of Air Force-level TCNOs (AFI33-138, 2005). This study will limit its scope of the TCNO process from initial TCNO dissemination (from the AFNOSC to the PMOs) to installation and subsequent compliance. As a result, the steps involved in TCNO generation will not be addressed. The AFNOSC disseminates TCNOs to NOSCs, NCCs, and "all Air Force program offices not administratively assigned to AFMC" (AFI22-138:20).

NOSC

Similarly, the Network Operations Center (NOSC) is responsible for acknowledging, disseminating, implementing, tracking and reporting TCNOs (AFI33-138, 2005:14). Air Force NOSCs reside at the MAJCOM level which report directly to the AFNOSC. As illustrated in figure 1, some PMOs fall under direct responsibility of the AFNOSC and receive their TCNO inputs accordingly. There are however, other MAJCOM-level PMOs that do not interact with the AFNOSC directly. The NOSC has the responsibility of disseminating implementing, tracking and reporting TCNO compliance for these PMOs. The NOSC "disseminates TCNOs to all NCCs within its AOR and to its MAJCOM-level PMOs and SPOs" (AFI33-138, 2005:21).

PMO

The Program Management Office (PMO) serves as the office of primary responsibility to process, evaluate, test, and coordinate TCNOs and risk mitigating countermeasures for those functional systems for which they are responsible. Furthermore, they "determine a TCNO's applicability, risks, vulnerabilities, and impact" to their programs and systems and "ensure there is a countermeasure developed for every applicable TCNO" (AFI33-138, 2005: 16). When a TCNO is released, it is the PMO's responsibility to determine if that vulnerability applies to the software on their system. If it does apply, the PMO must properly test that patch to ensure it will not unnecessarily disrupt the system. When the patch is deemed safe, the PMO gives notice to the appropriate agency (AFNOSC or NOSC) and either provides the patch to that agency or directly to a functional system administrator (FSA) for installation.

In some cases, the PMO must forward the TCNO to a Joint PMO for evaluation. This occurs when the program in question is not overseen by the Air Force or if the TCNO was not generated as the result of a DoD IAVA. For example, if JTF-GNO releases an IAVA to the Air Force, which in turn releases it as a TCNO, the joint PMO office has already verified the vulnerability patch at the JTF-GNO level and further coordination is not necessary. If however, the AFNOSC releases a TCNO based upon a vulnerability unique to the Air Force, the TCNO must be forwarded back to the joint PMO office to determine applicability and to conduct the appropriate testing before installation.

Per AFI33-138, there are five situations that PMOs must establish procedures for:

1) The TCNO does not apply to the program

2) The TCNO applies to the program and the FSAs are authorized to implement the countermeasure according to the procedures contained in the TCNO.

3) The TCNO applies to the program but the FSAs are not authorized to implement the countermeasure according to the procedures contained in the TCNO.

4) The TCNO applies to the program but actual implementation procedures are not yet available.

5) The applicability of the TCNO to the program is not known at this time.

For each of the above situations, the PMO must utilize the ENOSC web-based status page to maintain status information and notify the parent organization (MAJCOM or AFNOSC) as soon as applicability is determined.

NCC

The Network Control Center serves as the wing/base officer of primary responsibility to acknowledge, disseminate, and implement TCNOs and to track and report compliance with TCNOs (AFI-33-138, 2005: 15). While they are primarily focused on Air Force owned system compliance, NCCs often act as the reporting agency for PMOs that reside at a base or wing level. In some cases, NCCs have patching authority of the PMO asset, if that asset resides under NCC operational control.

FSA

Functional System Administrators are responsible for applying TCNOs to PMO assets. FSAs may receive their guidance and authorization to apply the TCNO patch from the NOSC, NCC or directly from the PMO depending upon the established agreement.

TCNO Composition

Every TCNO released by AFNOSC is assigned a priority and related suspense date. The priorities, which can be seen in Table 1, range from critical to low depending on the threat to the Air Force network the associated vulnerability has.

Table 1: Air Force TCNO priority categories

Priority	Description
Critical	Widespread and imminent/ongoing threat to the AFEN and supported operations
Serious	Widespread threat to the AFEN and supported operations is expected.
High	Threat to the AFEN and supported operations is likely
Medium	Threat to the AFEN is possible but is mitigated by such factors as difficulty of exploitation, limited deployment of vulnerable operating systems, etc.
Low	Threat to the AFEN is unlikely due to the assessed difficulty of exploiting the vulnerability

Source: Adapted from AFI33-138, Table 3.1

In addition, each TCNO will have multiple suspense dates dictated by the associated TCNO priority category. These dates can be seen in Table 2. The receipt acknowledgement date is the "date by which tasked organizations will acknowledge receipt of the TCNO to their next higher echelon" (AFI33-138:18). The initial

compliance statistics date is the "date by which tasked organizations will provide their first compliance statistics update to their next-higher echelon" (AFI33-138:18). This date is often omitted from NOSC released TCNOs. The compliance date is the "date by which tasked organizations must achieve full compliance with the implementation mandated by the TCNO" (AFI22-138:18). These suspense dates may also be influenced by the originating organization. For example, if JTF-GNO releases a vulnerability patch with a suspense date of 1 June, the AFNOSC will likely release its corresponding TCNO with a suspense date prior to 1 June, allowing adequate time to meet the JTF-GNO suspense. Similarly, the NOSC will release this same TCNO to its NCCs and PMOs with a suspense date prior to the AFNOSC date to ensure compliance.

Table 2: Air Force TCNO suspense dates

RULE	**A**	**B**	**C**	**D**
	If the TCNO priority is:	**then the**		
		receipt acknowledgment date will be	**initial compliance statistics date will be**	**compliance date will be**
1	Critical	£ 24 hrs after TCNO release	the first Monday after TCNO release	£ 15 days
2	Serious			£ 30 days
3	High			£ 45 days
4	Medium			£ 60 days
5	Low			

Source: Adapted from AFI33-138, Table 3.2

In order to effectively monitor the status of vulnerability patches across the Air Force, each TCNO is assigned a tracking number. The standard format for this tracking number is a four-digit year, followed by the three digit Julian date, and a three-digit

increment number (AFI-33-138). For example, the first TCNO released by the AFNOC on 19 January 2006 would be "TCNO AFNOSC 2006-19-001". Any revisions to this TCNO would result in appending this number with an alphabetical character. The first revision to the TCNO in this example would be annotated as "TCNO AFNOSC 2006-19-001a".

In addition to priorities, suspense dates and tracking numbers, TCNOs typically have implementation details which provide step-by-step implementation instructions, downtime estimates, projected risks and any other information deemed necessary to ensure proper compliance (AFI33-138, 2005:19). These implementation details are dictated by the TCNO generating organization, but may be augmented by other organizations (NOSCs, NCCs, PMOs) as deemed necessary.

Dissemination methods

Per AFI33-138, the AFNOSC will maintain a single distribution list of all Air Force units that receive AFNOSC-generated TCNOs (AFI33-138, 2005:20). In addition, TCNOs will be disseminated via secure electronic email (SIPRNET) and/or eTANG (AFI33-138, 2005:20).

Extensions

In some cases, extensions may be granted to PMOs in an effort to achieve full TCNO compliance. Extensions must have definite timeframes and the approving

authority depends upon the number of extensions previously granted for the TCNO (see Table 3).

Table 3: Air Force TCNO extension approval process

RULE	A If the extension requested is a	B And it is being requested by the	C Then it must be endorsed by the	D And the approval authority will be the
1	first extension	NCC	wing/base DAA	MAJCOM DAA
2		NOSC	first Colonel in NOSC chain of command	
3		FOA/DRU NCC/MSC	FOA/DRU DAA	
4		PMO/SPO	program manager	functional system DAA
5	second extension	NCC	wing/base DAA and MAJCOM DAA	AFNOSC Director
6		NOSC	MAJCOM DAA	
7		FOA/DRU NCC/MSC	FOA/DRU DAA	
8		PMO SPO	functional system DAA	
9	third extension	NCC	wing/base DAA and MAJCOM DAA	AFNETOPS/CC
10		NOSC	MAJCOM DAA	
11		FOA/DRU NCC/MSC	FOA/DRU DAA	
12		PMO/SPO	functional system DAA	

Source: Adapted from AFI33-138, Table 3.4

Compliance Reporting

TCNO compliance is realized when all actions directed in that TCNO are accomplished on all affected assets (AFI33-138, 2005:27). For each TCNO implemented

on a functional (PMO) system, a functional system administrator will record the following information (as outlined in section 3F of AFI33-138 dated 28 November 2005):

- The name, rank, unit, office symbol, phone number, and e-mail address for the person who implemented the TCNO.
- The Date receipt of the TCNO was acknowledged to the host NCC
- Exception details (if any), including any reason the TCNO was not accomplished as instructed
- The date compliance was achieved, verified, and reported to the host NCC.

MAJCOM Guidance

In addition to Air Force instructions, MAJCOMs may supplement their TCNO program guidance with additional written guidance. For example, Air Combat Command (ACC) released the Special Instructions to Communicators (Spin-C). This instruction applies to all NCCs that fall under direct control of ACC. Contained within the SPIN-C is a section that outlines the TCNO process mandated for ACC. This guidance is meant to complement the Air Force instruction with MAJCOM-specific instructions for TCNO dissemination, installation, reporting and tracking. The ACC guidance does specify the exclusion of AF-level PMOs, which are governed by AFNOSC guidance directly.

Pending Guidance

The Air Force is authoring a new guidance (currently in draft form) known as the Vulnerability Lifecycle Management System (VLMS) Concept of Operations (CONOPS). This document is meant to strengthen the procedures the Air Force currently

uses for securing its network in an effort to gain “improved centralization of command and control for AF Network Operations” (VLMS CONOPS, 2006:.2). Specifically the CONOPS is meant to “identify roles and responsibilities and operational requirements associated with the new Vulnerability Lifecycle Management System which will provide an automated way to “analyze the capabilities of existing USAF IT investments, identify gaps in capabilities, leverage current capabilities”, and achieve improved vulnerability and configuration management across the Air Force networks (VLMS CONOPS, 2006:2).

An admitted shortfall of this new plan is the fact that it does not mitigate the problem of manual patch installation that PMO systems present. Since PMO assets still rely on disparate processes that span multiple organizations, automation is not yet an option. In fact, according to the AFNOSC “most if not all PMO systems will be put into an “exceptions” list for remediation” (Matthews, 2006), and therefore will not benefit from such process improvements.

Accepted Patch Management practices

Patch (TCNO) management is a relatively new practice which has gained increased exposure over the last few years as computer technology and the need to protect the data contained within has crept into nearly every facet of organizational processes. Because it is in its relative infancy there is limited established theory on the subject. Instead, most literature addresses best practice ideas and recommended standards for implementing patch management in an organization. In addition, much of the recent literature on patch management addresses automated tools used to install these

patches, which in the case of this study are not applicable due to the complexities and varying testing procedures that PMO systems require. Accordingly, such environmental complexity has been classified as "a barrier to automated patch management" because of the need to determine the appropriateness of each patch and test the patch against each possible configuration (Colville, et al., 2002). In such instances, "enterprises need to recognize the impact that an unstructured environment has on their ability to rapidly deploy change with a confidence that unexpected results will not occur" (Colville, et al. 2002).

The remainder of the literature review will focus on literature as it pertains to the steps currently required for PMOs in an effort to determine recommended practices organizations follow in each. These steps are: dissemination, applicability assessment, testing, installation, and reporting. However, prior to undertaking these steps, there are two additional "best practices" echoed by numerous articles and industry professionals that apply to this study and bear mentioning: having a standardized process and maintaining an accurate system inventory.

Standardized Process

Devising an effective patch management program goes beyond identifying key roles and responsibilities. All written policies, procedures and tools must be standardized across the organization (GAO, 2003:12). Failing to do so introduces the risk of creating fragmented, ah-hoc processes and allowing subgroups within the organization to implement patch management differently or not at all (GAO, 2003:12). All such policies and procedures should be clearly documented and organized so that they can survive staff

turnover and resulting loss of institutional knowledge. This is especially true with personnel dependent processes such as applicability assessment and testing (Voldal, 2003). A key to ensuring standardization is having one, centralized organizational unit oversee the entire patch management process. Having a patch management process governed by decentralized units presents the unnecessary challenge of each unit devising its own methods and due to the resulting lack of standardization, often results in disparate processes and approaches (Barney, 2005). The requirement of standardized policies and procedures must apply to all internal and external organizations that interface with the network, a lesson NASA learned when implementing its own patch management system in 2004 (Jackson, 2005). In addition, there must be procedures in place to monitor and enforce these policies to ensure compliance (Jackson, 2005).

A major part of this standardized process is setting an agreed upon timeframe. As discussed in the previous chapter, all patches released by the Air Force are assigned a time frame for completion. Such a time frame is necessary to assure that the patch management process is not drawn out and left incomplete (Schouten, 2003). However, if the steps of this timeline are not efficiently ordered, the allotted timeframe may not be met. This timeframe is a large part of the measurement process of this study. In an effort to identify and disseminate leading performers' practices, an organization should as itself the following questions: "Is the organization responding in a timely fashion to alerts and patches? If not, why not, and what risks does this pose for the organization? What parts of the company are doing better than other parts and why?" (Brykczynski & Small, 2003)

Organizations "cannot succeed without establishing a well-defined process" for patch management (Brandman, 2005). As a 2004 GAO report points out, "Without consistent implementation of patch management practices, agencies are at increased risk of attacks that exploit software vulnerabilities on their systems" (GAO, 2004:11).

Accurate system inventory

As the old saying states, "You cannot manage what you don't know." This concept is a summary of Lord Kelvin's statement "I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be" (Kelvin, 1883). Therefore, in order for a patch management plan to be comprehensive and effective, the devices that it supports must be known. Accordingly, experts recommend collecting and actively maintaining an active IT inventory of every machine in the organization (Chan, 2003). This is not limited to user workstations, but includes every single device that has an embedded computer device (Chan, 2003:6). While the content and level of detail of the information collected for each device may vary slightly among organizations, the National Institute of Standards and Technology recommends, at a minimum, collecting information regarding the device's hardware, operating system and any major applications that reside on that device (Mell & Tracy, 2002:26). While this is an admittedly daunting task for large, heterogeneous organizations, it is necessary to understanding the possible complications caused by a

complex and expansive computer environment. Because it is such a large undertaking, automated tools and software packages are frequently used to collect this data (Roberge, 2004: 8).

Aside from providing an overall idea of what systems and related vulnerabilities exist on an organization's network, an accurate system inventory provides the means to categorize and prioritize patching based upon system threat level, vulnerability, and criticality (Mell & Tracy, 2002:26). A systems threat level is dictated by its potential to cause harm to another system or the network (Mell & Tracy, 2002:26). Systems that face high threat levels are usually those that are accessible to external users such as Web or email servers or those that contain critical or sensitive information such as financial, personnel or proprietary information. A vulnerable system is one that has a "flaw, misconfiguration, or weakness that allows the security of the system to be violated" (Mell & Tracy, 2002:26). Web servers often introduce vulnerabilities due to their relative ease of access from external users. A system's criticality is measured by its importance to the organization (Mell & Tracy, 2002:26). By identifying those systems that impose a high level of threat to the network, are highly vulnerable and are critical, an organization can prioritize its assets and determine which should be patched first. In addition, an inventory provides the means to determine which patches are applicable to which machines and who is responsible for them (GAO, 2003:12). Unlike the inventory process, categorization and prioritization is very difficult to automate because assigning a priority is often a subjective process dictated by organizational practices and personnel expertise (Roberge, 2004: 8).

An accurate system inventory also acts as a change catalyst (Wrenn, 2004). For example, frequent inventories will identify laptops and other portable devices that intermittently connect to the network (Wrenn, 20004). They also provide a means to identify aging or unique operating systems and software products, recognize opportunities to further standardize network assets and in turn, reduce the number of vulnerabilities and ease of patching process (Wrenn, 2004).

Finally, asset management must be a continuous process. Hardware, software and system configurations are frequently updated, added or removed and the inventory must reflect these changes (Barney, 2005).

TCNO Dissemination

The underlying goal of an effective dissemination process is to produce an efficient method of quickly deploying a security patch to the organization (Dadzie, J, 2005). Dissemination includes both the method(s) used for deploying the patch as well as the timeframe in which the patch is distributed.

The timeliness of the security patch dissemination process is what determines the level of risk the organization faces (Schwartz, 2004). Automated patch distribution can make the patch dissemination process less cumbersome. However, automation generally works best in organizations with a heterogeneous environment with standardized configurations (Mell, 2002). As previously discussed, Air Force PMOs systems are not standardized and therefore cannot be automatically updated. Those organizations that cannot automate their patch dissemination must rely on alternate methods (Voldal, 2003). For example, to disseminate to its unmanaged clients, Microsoft uses a corporate-wide

email system to provide information and links to its security patches which are located in a centralized location for download (Alliegro, 2003).

In most organizational patch management environments, patch dissemination occurs after assessment and testing and is part of the installation process. However, per Air Force Instruction, the TCNO must be distributed to PMOs from the AFNOSC, and subsequently from a MAJCOM (if applicable) before PMOs can begin any assessment or testing. Recent research examined the Air Force's patch management process (Kubinsky, 2004), in which the author identifies potential shortfalls including the PMO patch distribution being out of sequence. He suggests that rather than PMOs assessing applicability and testing TCNOs after they are released, these steps should be moved to the beginning of the process so that they can be conducted in conjunction with associated AF testing.

Assessment

Prior to the testing and implementation process, experts highlight the importance of assessing the risk of the patch and determining if it is applicable to the system in question (Schouten, 2003). If a given vulnerability applies to something that does not exist on the network in question, there is no need to patch (Barney, 2005). For example, if the vulnerability applies to Microsoft Windows and the system does not run the Windows operating system, the vulnerability patch is not likely to be applicable. This is where an accurate system inventory will prove helpful. Knowing what exists in the organization allows administrators to determine if a security patch will apply to the patching environment. Only deploying those patches that are relevant to the

organizational environment will decrease the overhead and effort required to maintain security (Microsoft, 2006).

An additional aspect to consider when assessing a security patch is whether the organization wants to assume the risk of installing the patch. Many security patches require reboots and machine downtime. Often the systems being patched are considered operationally critical and any considerable downtime could prove costly. These costs must be weighed against the risk imposed by the vulnerability. Organizations should have a risk assessment standard to use when making such decisions (Chan, 2003). A widely held view by experts is that the cost of implementing a patch should be less than the risk posed by its vulnerability (Barker, 2006). To properly assess the risk of a security patch prior to installation, an organization should consider the importance of the system, the criticality of the vulnerability and the risk of applying the patch (GAO, 2003:12).

Testing in a heterogeneous environment

Testing is a necessary step in the patch management process. Failure to properly test a patch can result in unanticipated damage to the confidentiality, integrity and availability to an organization's network, systems or data (Grigg & Oleksak, 2004). To illustrate the importance of testing, consider the fact that 90% of the companies who did not test patches before they were deployed on production systems reported system outages (Perez, 2001). Because the numerous and diverse PMO systems contribute to the heterogeneous nature of the Air Force network, a "one-size fits all" approach to patch management is not feasible. Such a complex environment increases the need for proper

testing prior to patch release. In a highly structured environment, a system update can be tested once and widely deployed. However, in a complex environment there is more overhead and delay associated with quality assurance testing (Colville, et al., 2002).

While testing is necessary, it must be controlled and specified in advance so that it can be built into the overall process and timeframes can be anticipated. Testing procedures should be part of an overall testing plan that is comprehensive, yet generalized enough to be followed for every new patch encountered (Walther, 2004). To accomplish this, some companies maintain virtual machines on which administrators can pre-install and pre-configure test environments with different system configurations, and store them in a mass storage, saving time, necessary personnel and resources (Chang, et al., 2005).

A test environment should mimic the production environment as close as possible, with every type of platform in the organization represented (Voldal, 2003). Also, those involved in the testing process should have expertise in mission critical systems and possess the ability to verify the stability of those systems after the patch is installed (Voldal, 2003). When testing an organization should follow some important steps (Grigg & Oleksak, 2004):

- Always verify the source
- Always virus scan the patch
- Ensure the patch: corrects the vulnerability, does not open an old vulnerability, does not introduce a new vulnerability, does not degrade system performance and is compatible with all other required applications.

Organizations should have a contingent plan in case the security patch causes unwanted damage (Chan, 2003). This contingent plan must also be tested to ensure timely remediation (Chan, 2003). The testing process can add unwanted time to the overall patch management process. While patches are being tested, organization should be aware of possible workarounds to provide temporary remediation until the patch is ready for deployment (GAO, 2003:13).

If, after testing the patch, it is deemed to risky to install the patch across the organization, the details of the decision should be formally documented for future reference (Grigg & Oleksak, 2004).

Installation

While a large part of the installation process actually has to do with distribution, which has already been addressed, there are some additional considerations that organizations should consider. As was previously addressed, automated installation is often not possible with PMO systems, so manual installation methods are necessary. Since manual installation relies on administrators at remote locations, it is imperative that a security patch have detailed installation instructions (Grigg & Oleksak, 2004). In an effort to ensure a level of control and standardization, organizations may want to consider instituting technical and/or procedural controls to ensure only certain individuals may install security patches (Chan, 2004).

Security patching often involves system reboots and resulting system disruptions. Therefore organizations should consider scheduling their patch installations after peak business hours, especially for mission-critical systems. Prior to patch installation,

administrators may also want to consider backing up the systems to allow for restoration in case of an error during installation (Mell & Tracy, 2002).

Reporting

Again, because most organizations are migrating towards an automated patch management solution, much recent literature focuses on automated reporting tools that communicate patch installation progress and success. However, there are important points to consider no matter what the patching process is.

Some experts recommend using a standardized form and an online system to report patching status (Nicastro, 2003). This provides system administrators with the ability to report in an efficient manner as well as a consolidated means to track patching compliance in a distributed environment. That being said, there should also be procedures in place to review this information on a regular basis to ensure compliance (Nicastro, 2003).

Part of an effective reporting process includes maintaining good communication amongst all involved parties. "All people involved in patch management in the organization should maintain good communication channels among them" (Chan, 2003). Everybody has to know his/her roles and responsibilities, what to do, and how to do it, so that no step of a process is missed. This is particularly important for global organizations such as the Air Force who have worldwide heterogeneous networks and computing sites (Chan, 2003).

Summary

This chapter examined applicable regulations that govern the Air Force TCNO process to provide a basic understanding of the process that Air Force organizations and PMOs must adhere to when conducting patch management. In addition, the major steps of a successful patch management program were examined to provide a thorough understanding of the process and introduce some commonly used “best practices” among various organizations.

III. Methodology

Chapter Overview

This chapter discusses the methodology used for this research. Specifically, it will address the type of design to be used, the study's questions, units of analysis, data collection and data analysis strategies employed and the methods used to achieve validity.

Type of design

As illustrated by the research questions first presented in Chapter 1, the purpose of this research is to examine existing processes in used by PMOs with assets residing on the Air Force network and ultimately provide recommendations to improve existing PMO patch management methods. The exploratory nature of this research is well suited to a multiple case study design. Case study research is particularly appropriate for "sticky, practice-based problems where the experiences of the actors are important and the context of action is critical" (Benbasat, et al, 1987). As this chapter will illustrate, the findings of this research will be derived directly from the implemented policies, practices and insight garnered directly from the research participants.

The underlying goal of this research is to attempt to determine some differences in the way PMOs with shorter TCNO compliance rates operate compared to those PMOs with longer compliance rates. Therefore, using a multiple-case design with theoretical replication is ideal. Theoretical replication allows for the comparing and contrasting of multiple cases in order to find varying results for predictable reasons (Yin, 2003). For

example, those PMOs with a shorter compliance timelines might have an explicitly defined testing process with set deadlines, whereas PMOs with longer compliance timelines do not. Theoretical replication benefits from a case study design using 4 to 6 cases (Yin, 2003). Therefore, this case study design will examine 4 separate PMO organizations. The method of selection for these PMOs is discussed in the *Units of Analysis* section of this chapter.

Yin (2003) outlines five important concepts of a case study research design:

1. a study's questions
2. it propositions, if any;
3. its unit(s) of analysis;
4. the logic linking the data to the propositions; and
5. the criteria for interpreting the findings.

All five concepts will be addressed in this chapter. Take note however, for the sake of clarity, the fifth concept (interpretation criteria) will be addressed following a discussion of the data collection strategies to be used in this study.

A study's questions

Yin provides a basic categorization scheme for the types of research questions that lend themselves to case study research: "who," "what," "where," "how," and "why." For clarity, the research questions for this study are again listed below:

RQ1). How does the lack of standardized, centrally managed, and enforced TCNO patching procedures for PMO impact the TCNO compliance timeframe and in turn, the security posture of the Air Force Network?

SRQ1). How do the methods of TCNO distribution (both to and from the PMOs) impact the TCNO compliance timeframe?

SRQ2). How do PMO applicability assessment methods impact the TCNO compliance timeframe?

SRQ3). How do PMO testing methods impact the TCNO compliance timeframe?

SRQ4). How do PMO patching methods impact the TCNO compliance timeframe?

SRQ5). How do PMO reporting methods impact the TCNO compliance timeframe?

SRQ6). Are there any additional organizational behavior issues that might impact the TCNO compliance timeframe?

As can be seen, the above questions are in the "how" form. Although Yin would suggest that "how" questions typically are explanatory in nature, as previously stated, the design of this case study is exploratory. That is not to say however, that the use of "how" questions in exploratory study design is uncommon. In fact, a ten year study focusing on the use of case research in information systems found that the majority of case studies that posed "how" questions were exploratory in nature (Dube & Pare, 2001).

Study propositions

Propositions are meant to direct attention to something that should be examined within the scope of the study (Yin, 2003). The purpose of this research is clearly stated and the research questions, which are based upon actions mandated by Air Force regulation, are designed to provide the focus and direction that propositions are meant to provide. That being said there are four additional propositions that can be made based on the purpose of this study as listed below:

Proposition 1). High performing organizations have an accurate system inventory

Proposition 2). Despite a possible similarity in TCNO compliance results, due to the lack of standardized TCNO processes, the methods of process execution will vary amongst all PMO organizations studied.

Proposition 3). There will be noticeable difference in the TCNO processes (or the execution of those processes) of high-performing and low-performing PMO organizations

The first proposition addresses a key point made in Chapter II, which identifies having an accurate system inventory as being a key step in a successful patch management process. Therefore, it would stand to reason that an organization that has a successful TCNO process would also have an accurate system inventory. Since this important point is not addressed directly in the research questions, it is important to highlight here to ensure it receives proper attention throughout the course of this research effort. The second proposition predicts that a lack of process standardization and centralized control will cause significant variation in the execution of TCNO processes amongst the PMOs studied for this research. The third proposition states that although processes will vary amongst all PMOs studied, something about them or their methods of execution will distinguish the high performing from the low-performing organizations.

Unit(s) of analysis

The problem of this thesis addresses TCNO programs at an organizational (PMO) level. Therefore, the unit of analysis for this study will be a PMO. That being said, data collection from individuals that operate within and in conjunction with these organizations will be necessary as these entities play a critical role in the success of the PMO TCNO process. This data collection will be limited to those directly involved with the PMO TCNO process as is required to fully understand the organizational processes.

It may also be necessary to collect some degree of information from additional organizations that directly interact with PMOs in the context of the TCNO process. The organizational units of analysis will consist of a representation of Air Force PMOs. This will be limited to MAJCOMs or the AFNOSC, from which the PMO receives its TCNOs.

Selection of the PMOs (and subsequent individuals) to study will depend on the initial data analysis. To conduct this data analysis, an initial set of MAJCOM TCNO historical data will be statistically analyzed, to identify those PMOs with the best and worst average compliance rates. MAJCOMs used for this initial data collection will be chosen based upon similarities of policies, procedures, and organizational size. The type of information to be collected is specified later in this chapter.

Once this initial set of data is analyzed, two PMOs will be selected from each MAJCOM, one that is identified as performing well (with the best compliance timeframes) and one that has a noticeably longer TCNO implementation time frame. When selecting these four PMOs for further study, similarity in organizational size as well as the number and type of systems deployed on the AF network will be taken into consideration.

Data collection strategies

A case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations) (Benbasat, et al, 1987).

One of the inherent problems with not having a standardized process to manage the TCNO process amongst PMOs is the lack of consolidated metrics and other

compliance data pertaining to the installation of PMO related TCNOs. As a result, data collection will be a structured effort that addresses each major entity involved in the process, from the base level functional administrators and Network Control Center Personnel that install the TCNOs on the PMO assets, to the MAJCOM and AF level Network Operation Centers (NOSCs) which distribute TCNOs and report on their compliance.

In order to gain a basic understanding of the Air Force PMO patch management landscape, data will first be collected to answer the following questions: "How many PMOs are connected to the AF network?" "How many PMO machines are on the AF network?", "What are the functions and priority levels of PMO assets on the AF network?", and "How many total machines comprise the AF network?" Obtaining this data may prove difficult. Based on conversations with the AFNOSC, since not all PMOs are registered with the TCNO dashboard, there is no single record of Air Force PMOs or their respective systems. Although not consolidated, this data should be available from the AFNOSC and the various AF MAJCOM NOSCs. Knowing this basic information should provide enough information to measure the impact non-compliant PMO machines can have on Air Force network security.

Multiple data collection methods are typically employed in case studies research (Benbasat, et al., 1987) and this will be no exception. Yin identifies several sources of evidence that lend themselves to case study research including documentation, archival records, and interviews all of which will be used in this case study (Yin, 1984).

Documentation

In the context of case studies, documentation is useful for augmenting and corroborating evidence from other sources (Yin, 2003). Just as useful, often documentation will not corroborate, but rather contradict evidence presented by other sources. In such cases, further investigation should be conducted to determine the underlying facts (Yin, 2003).

For the purposes of this research, documentation will be required from both the Air Force as well as the PMOs of interest. Current documentation on Air Force TCNO processes and procedures while limited in content and dispersed across various regulations spanning from Air Force level agencies to individual MAJCOMs, provide a picture of how much of the process should be occurring. It is important to understand these processes and ensure that all written procedures complement rather than contradict each other. Once the Air Force process is understood and outlined, the same will be done for the PMOs of interest. Studying their written policies and procedures for TCNO testing and implementation (from the time of receipt from the appropriate AF level organization to the time of deployment) should provide some insight as to how various PMOs vary in their methods.

Archival Records

Archival records can come in both electronic and hard copy form, however their usefulness often varies between case studies (Yin, 2003). Archival records in the form of past TCNO compliance data will be imperative to this research for two reasons. First, they will provide a measurement of how secure (or insecure) the AF network was at any

given time, due to non-compliant systems. Second, this data will provide a timeline detailing initial release of the TCNO, receipt by the PMO, release of follow up TCNO by PMO (if applicable) and subsequent patching of machines, both PMO and Air Force. This will provide a good means for comparing patch deployment timeframes between Air Force and PMO entities. Each MAJCOM archives this data electronically. Because this information is so dispersed and non-standardized, examining all of the TCNO data across the Air Force would be unrealistic. Instead, two MAJCOMs will be selected and data on all TCNOs released within the last 5 years will be collected. Not all TCNOs apply to all machines and most are software specific. Therefore, data collection will be limited to only those TCNOs that affect both AF and PMO systems. For each TCNO, specific criteria will be collected: Priority of TCNO, number of days between AF and PMO release (the time the PMO receives the patch to the time they release it for installation) and the disparity between AF and PMO compliance rates. This will not only identify historical PMO process timeframes and compliance rates but will also provide a means to compare these rates to Air Force rates.

What this data will not show is the testing process used by the PMOs. This information will be gathered through documentation as previously mentioned, as well as through interviews of personnel involved in the PMO TCNO process.

Interviews

Interviews will be conducted with both AF and PMO personnel. The first interview will be with the AFNOSC, as this is the entity responsible for developing the procedures and methods to attain TCNO compliance for the Air Force. The AFNOSC

dictates and enforces any new policy that would standardize and govern PMO TCNO testing and deployment. In addition to reporting compliance, it is developing new policy and methods that will govern the TCNO process for the entire Air Force. Therefore, it has a good high-level view of the problems that the Air Force is facing with PMO TCNO patching and should provide good contacts for further interviews and research. Additionally, it is this office that is guiding the focus of this research, providing advice on scoping the problem as new issues arise. In addition to the AFSNOC, interviews will be conducted at the NOSC and base levels to capture the PMO-related processes that occur at each. Since NOSCs have the responsibility of notifying and reporting compliance of all PMO-related TCNO patches within their control, they should be able to provide methods both formal and informal that are used to track this information internally, as well providing other sources of data collection (additional documentation and archival data) that may shed some light on the process. Similarly, it is the NCC's responsibility to ensure compliance of base level PMO TCNO patches and report this compliance to the respective MAJCOM. The individuals at these locations often have the most personal interaction with the FSAs responsible for loading TCNO patches on PMO machines and in the cases of some systems, may even act as the responsible FSA. Once PMOs are selected based upon the initial data analysis, interviews will be conducted at the policy (PMO office) and implementation levels (FSAs) of the process to get an adequate view of the entire process. These interviews will be focused and semi-structured in design to provide participants the opportunity to interject information when they deem necessary while still allowing the researcher to guide the process with pre-

determined interview questions. This initial set of interview questions is included in the Case Study Protocol found in Appendix A.

In an effort to gain adequate information to answer the sub-research questions (and ultimately the main research question), the data collection process must be detailed enough to gather specifics on each process in question. Examples include determining the number of people involved in the process approval chain, whether there is a defined process schedule, levels of training and other items that may have an influence on the process timeline.

Data analysis strategies

Using multiple data collection methods provides a means for using triangulation to support the research questions, which in turn leads to a richer data analysis (Leedy & Ormrod, 2005). For this exploratory case study, a cross-case synthesis analysis technique will be used. With this strategy, will employ the use of a word table, which will be used to compare and contrast various aspects of the case study objectives as defined in the research questions. The goal of a cross-case synthesis is to uncover patterns in the data that might ultimately lead to conclusions. To conduct this analysis, PMOs selected for this study based on the criteria previously described will be compared once all data is collected. The data will be organized by unit of analysis, in a method that facilitates comparison. Data will be grouped by sub-research questions for ease of interpretation. This should allow for easier identification of patterns contained within the data. The data will be synthesized and conclusions will be made based upon critical interpretation. It is important to note that this form of analysis often relies heavily on argumentative

interpretation rather than numeric calculations, which is more subjective in nature (Yin, 2003). That being said, if the data allows, it may be possible to conduct a statistical analysis using a Chi Square analysis or similar method; however at this point it is difficult to determine whether the data will be too qualitative to employ statistical methods.

Methods of achieving validity

According to Yin (2003), the quality of a research design can be determined by four tests of validity: Construct Validity, Internal Validity, External Validity and Reliability. Each will be addressed further below:

Construct Validity

Construct validity involves establishing correct operational measures for the concepts being studied (Yin, 2003). Often the perceived subjective nature of case studies proves difficult to ensure construct validity. However, there are some tactics that can be used to bolster this in a research design including using multiple sources of evidence, having key informants review the draft case study report, and establishing a chain of evidence (Yin, 2003).

Collecting information from multiple sources of evidence allows for triangulation of the data sources, resulting in converging lines of inquiry (Yin, 2003). This will likely further support the findings and accuracy of the study. As previously outlined in data collection strategies section of this chapter, evidence will be collected from documentation, archival records and interviews, thereby utilizing multiple sources of evidence and in turn, bolstering construct validity.

Having informants review the draft case study report is intended to support the factual contents of the report. A draft of this case study will be sent for review to all key research participants so that factual data contained within can be verified prior to finalization and publishing of the document. Key research participants will include all interviewees from which data was collected to generate conclusions. During this process, reviewers will examine the factual data contained within the case study report and submit comments as necessary. Any comments that suggest factual data is misrepresented will lead to further evidence gathering until the reviewer is satisfied. While this process may not result in complete agreement in amongst the reviewers regarding the researcher's final conclusions, it should support the facts which are used to produce this studies' findings (Yin, 2003).

Internal Validity

According to Yin (2003), "internal validity is only a concern for explanatory case studies". Since this is an exploratory case study design, internal validity will not be addressed further in this methodology discussion.

External Validity

External Validity determines whether a study's findings are generalizable outside its immediate context (Yin, 2003). The use of replication logic in a multiple case study design is a tactic to reinforce external validity. By generating conclusions from data gathered from multiple case studies, the findings of this case study should be adequately supported by external validity.

Reliability

The goal of ensuring reliability is for investigators conducting the same case study using the same procedures to arrive at the same conclusions (Yin, 2003). Two tactics can be used to increase the reliability of a study: the use of a case study protocol and the use of a case study database. This research will employ the use of both tactics.

The case study protocol is a tool designed to keep the researcher focused on the subject of the study as well as anticipate and prepare for potential problems (Yin, 2003). Yin (2003) suggests a case study protocol should have the following elements:

- An overview of the case study project: objectives, background, relevant readings
- Field procedures to be used: gaining access to sites, procedural reminders, etc.
- Case Study Questions: the specific questions a researcher must keep in mind while conducting the research
- A guide for the case study report: outline, data format, bibliographical information

Aside from the last item, a guide for the case study report, which is dictated by the Air Force Institute of Technology formatting standards, the case study protocol for this research contains all of these items. Field procedures including those to use prior, during and after interviews are included in this document. Outlining these procedures allows for duplication of the process, regardless of the researcher. This is especially important in a multiple case design such as this one. Due to its length, the case study protocol for this case study can be found in Appendix A.

A case study database is meant to be a collection point for all of the raw data and information collected during the course of the investigation process of the research study. This may include case study notes, documents, quantitative tabular materials and narratives (Yin, 2003). The database design for this research effort can be found in Appendix A.

Overview of the Interview Process

Semi-structured interviews were conducted with individuals directly involved in the PMO TCNO process from distribution to implementation and compliance reporting. Since the roles of the individuals varied, so to did the information that was gathered from each. Therefore, each type of interviewee warranted a unique set of questions. A complete list of these questions are contained within the Case Study Protocol found in Appendix A)

Summary

This chapter outlined the methodology used to conduct the research. Specifically it outlined the case study approach, addressing the integral parts of case study as well as identifying data collection and analysis strategies and methods for achieving validity. Finally, a brief overview of the interview process was provided, which will be expounded upon in greater detail the following chapter.

IV. Analysis and Results

Overview

This chapter will present the analysis of the collected data and the results of the research. Specifically, the initial data collected for the purposes of site selection will be described in detail the results of the analysis discussed. Then, the site selection process will be outlined briefly. Following, the interview results will be analyzed, compared and contrasted amongst the various sites to illustrate the processes used by each organization.

Initial Data Collection and Analysis

As mentioned in the previous chapter, to facilitate an effective unit of analysis selection process, an initial set of TCNO historical data was to be statistically analyzed in order to identify those PMOs with the highest and lowest average compliance rates. A database containing this historical data was provided by the AFNOSC. (The basic structure of the tables from this database used for initial data collection along with the SQL commands written to extract the data can be found in Appendix B). This database contained five years of PMO TCNO compliance data (2001 to 2006) with a total of 751 unique PMO entries. However, many of these entries were repetitive, blank, incomplete and unintelligible and as a result, had to be combined or excluded from data analysis. Entries such as “XXX”, “9”, “PMO”, “Test” “Local PMO issues” and “none” could not be attributed to an existing Air Force PMO. There were also entries such as “MS Windows” and “Office XP”, which are applications and not PMOs and thus could not be analyzed as such. In addition, there were entries such as “Geobase” and “CE-Geobase”,

which while indicating the same system, are treated as separate entries in the database due to their unique spellings and formatting. In fact, for one particular PMO there were over 42 different variations in spelling for the PMO name, causing 42 different database entries. The historical data for these entries had to be manually combined as carefully as possible so that accurate performance measurements could be taken. Some entries contained organizational units rather than PMO names. For example PMO entries of "CES" and "CONS", which while valid organizational units, do not indicate valid PMO names. Following the adjustment of the database to compensate for these extraneous entries, there were a total of 424 PMO entries. From these remaining entries in the database, a key set of data and statistics were gathered for analysis and final selection. These statistics can be broken down into three main categories: *descriptive*, *performance* and *impact on network security*.

Descriptive Statistics

These statistics were gathered for descriptive purposes and were not used to illustrate a PMO's performance. In doing so, they were also used to eliminate PMOs from further data analysis if certain criteria were not met. The descriptive statistics gathered for this study were: *total patches*, *number of units*, and *number of TCNOs*.

Total Patches: This is a measure of **total work** for each PMO. It is the sum total of patches a PMO was tasked to install over the data collection period for all TCNOS where number of applicable PMO assets (machines) is greater than one. This number does not necessarily represent the number of machines a PMO has deployed on the Air Force network. For example, a PMO had two applicable TCNOs over the five year

period. The first TCNO affected six of the PMO's assets and the second affected eight PMO assets. In this example this PMO had fourteen total patches. This situation, while purely hypothetical, is representative of the provided data and also raises an important issue: the number of machines each PMO actually has deployed on the Air Force network is not data that is readily available, nor can it be derived from the provided database. There is no way to tell from the provided data whether the PMO has a total of eight assets or if it had ninety but no more than eight were affected by these TCNOs. The only thing that can be determined is that this particular PMO has *at least* eight assets on the Air Force Network. Therefore, Total Patches while an accurate measure of total work does not provide a complete picture of the PMO asset landscape. This measure was also used to eliminate extraneous data points. PMOs with a *Total Patches* value of less than one were eliminated from the data set as they would have no performance data to measure. Following this elimination process, there were 240 PMOs remaining.

Number of Units: This is a measure of **geographic scope**. It represents the number of bases at which each PMO has TCNO-applicable assets. This number was also used to eliminate extraneous data points as any PMO that has a *Number of Units* value less than two, was removed from the data set. The rationale behind this was as follows. If a PMO is a poor performer at a single location, it may be due to existing circumstances (policy, procedures, infrastructure, etc) at that particular base and have little to do with the PMO itself. If on the other hand, a PMO exists at a number of bases and is exhibiting poor performance at multiple locations, there is a greater chance that the issues exist at the PMO level rather than the base level. While eliminating such PMOs from the data set

does not eliminate base-level issues, it does reduce the chances of such issues being the sole influence over TCNO compliance. Following this removal process, there were a total of 70 PMOs remaining to be included in the analysis.

Number of TCNOs: This is a measure of the applicable TCNOs for each PMO. Each TCNO for which a PMO had one or more applicable assets adds to the cumulative total of TCNOs for that PMO. This descriptive statistic was used to calculate the performance statistic *Average Days Overdue per TCNO* (see below).

The list was once again scrutinized to eliminate any extraneous or invalid names, which resulted in the removal of 24 additional entries, resulting in a list of 46 PMOs to be included in the historical performance analysis.

Performance Statistics

These statistics were used to rank order and in conjunction with the *impact on network* security statistics, ultimately select the highest and lowest performing PMOs based on a number of performance related categories. The performance statistics used in this study were: average days overdue per TCNO, percent of overdue TCNOs, number of non-compliant TCNOs, and percent of non-compliant TCNOs.

Average Days Overdue per TCNO: This is a performance measure of how many days overdue a PMO averages for each of its applicable TCNOs. It was calculated by dividing a PMO's total number of days overdue for each TCNO by the *Number of TCNOs* for that PMO. This figure provides a statistical average of a PMO's performance. Recall, *overdue* indicates the TCNO was at some point in time, past the compliance due

date provided in the TCNO. For the purposes of this data analysis, *overdue* is different than *non-compliant* (see below).

Number of Non-Compliant TCNOs: This is a measure of both performance and to some extent, existing vulnerability. For the purposes of this data analysis, *non-compliant* means past the compliance due date provided in the TCNO and not patched. It is important to remember that a TCNO could have been overdue, even for a number of months or years, but if it has since been patched, it is now considered compliant. For this reason, simply looking at the overdue or non-compliance data in isolation could be misleading. An organization might be 100% compliant to date, but the time it took to comply with those TCNO may have consistently exceeded the mandated compliance date, which in reality points to poor patching performance.

Percent Overdue TCNOs: This measure of performance represents what percent of a PMO's total number of applicable TCNOs were overdue. It was calculated by dividing number of overdue TCNOs by the total *number of TCNOs*. Using a percentage for this performance statistic takes into account the total applicable TCNOs for each PMO and allows all PMOs to be analyzed equally. For example, if PMO1 had two overdue TCNOs and PMO2 had 8, at face value, PMO1 was the better performer. However, if PMO1 only had two applicable TCNOs over the five year period whereas PMO2 had 100, clearly PMO2's 8% overdue statistic is far better than PMO1's 100% overdue statistic.

Percent of Non-Compliant TCNOs: This measure of performance represents what percent of a PMO's total number of applicable TCNOs were still non-compliant at the

time of data collection. Using a percentage for this performance statistic takes into account the total applicable TCNOs for each PMO and allows all PMOs to be analyzed equally. However, note that contrary to the overdue statistic, the raw number of non-compliant TCNOs was used to analyze a PMO's performance. This is due to the fact that any rate of non-compliance is considered an existing security vulnerability and was therefore weighted heavier in the analysis of PMO performance.

Impact on Network Security Statistics

While nearly all of the performance-based statistics previously discussed can be considered network security vulnerabilities, two statistics in particular illustrate the overall impact an individual PMO has had on Air Force network security. These statistics are: Number of overdue or non-compliant TCNOs with a rating of "Serious" or "Critical" and "Number of non-compliant patches".

Number of Overdue or Non-Compliant TCNOs with a priority of "Serious" or "Critical": As discussed in Chapter 2, each TCNO is given a priority to both illustrate its threat level and to determine its mandatory compliance date, the two most severe of which are "Serious" and "Critical". This statistic represents the number of TCNOs with either priority a PMO allowed to become overdue or remain non-compliant.

Number of Non-Compliant Patches: This is a measure of total existing vulnerability. It represents the number of vulnerabilities for each PMO that remain un-patched at the time of data collection. This figure was calculated by multiplying a PMO's *Number of Non-Compliant TCNOs* by the existing number of non-compliant patches for each of those TCNOs.

Site Selection

In order to follow Human Subjects Research Guidelines and mask PMO identities, each PMO was assigned a unique number for identification. The statistics identified in the previous section were calculated for each PMO in the database. Each PMO ID was listed on a spreadsheet with their associated values of each of the statistics. These values were then used to rank order the PMOs within each statistic to determine the best and worst performers. A matrix-style chart was used to plot the ranks of the PMOs and their associated ranks for each category. These rankings can be found in Appendix B. The rankings for each category were added, assigning each PMO a "score". The two PMO with the lowest scores in both the lowest and highest performing matrix charts were selected for further study. The statistics for these four PMOs can be seen below.

Table 4: PMO Site Selection and Performance Data

Top 2 Highest Performing PMOs																
This table contains data on the two highest performing PMOs determined from data analysis. These PMOs will be used for final data analysis. The complete list of rank ordered PMOs and their associated values can be found in Appendix D.																
	Network Security Impact						Performance Measures						Descriptive Data			
PMO #	Least Non-Compliant Patches		Least Non-Compliant TCNOs		Least "Serious" or "Critical" Overdue/Non-Compliant TCNOs"		Least Days Overdue Per TCNO		Lowest % Non Compliant TCNOs		Lowest % Overdue TCNOs Total		Highest Workload (Most Total Patches)		Most Dispersed (# Units)	
	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value
5	1	0	1	0	2	1	8	34.5	1	0%	4	33.33%	33	67	10	3
10	1	0	1	0	2	1	22	85.61	1	0%	3	16.67%	35	61	11	2

Table 5: PMO Site Selection and Performance Data

Top 2 Lowest Performing PMOs																
This table contains data on the two lowest performing PMOs determined from data analysis. These PMOs will be used for final data analysis. The complete list of rank ordered PMOs and their associated values can be found in Appendix D.																
	Network Security Impact						Performance Measures						Descriptive Data			
PMO #	Most Non-Compliant Patches		Most Non-Compliant TCNOs		Most "Serious" or "Critical" Overdue/Non-Compliant TCNOs"		Most Days Overdue Per TCNO		Highest % Non Compliant TCNOs		Highest % Overdue TCNOs Total		Highest Workload (Most Total Patches)		Most Dispersed	
	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value	Rank	Value
9	5	312	2	56	1	89	10	181.7	7	30.94%	9	91.16%	3	10,897	2	67
16	1	1411	1	93	2	70	24	92.85	3	62.84%	15	88.51%	1	27,263	1	77

Interviewee Participants

In all, 12 individuals were interviewed. These 12 individuals were involved in one or more the various processes of TCNO administration for each PMO, from testing to implementation. In addition, four of the interviewees were involved at a MAJCOM NOSC or NCC level, responsible not for a single PMO, but for overseeing the overall TCNO program for that entity. This information was important to capture since these individuals enforce and manage many of the processes PMOs that interact at those levels are required to follow. The interview pool was comprised of both military and civilian with an average of 2.45 years experience working with the Air Force TCNO process. Within each organization, each interviewee was assigned a number in succession. This number coupled with an organizational identifier was used as a composite interviewee identifier (as shown in Table 6).

Table 6: PMO Interviewee Information

PMO Interviewee Information				
Interviewee ID	**Job Description**	**Role in TCNO process**	**Experience with Air Force TCNO process**	**Familiar with AFI 33-138?**
05_01	Programmer	Acknowledgement, Applicability Assessment, Testing, Installation, Reporting	Eight Months	Yes
10_01	Software Engineer	Testing	Two Years	No
10_02	IT Specialist	Applicability Assessment, Installation, Reporting	Eight Years	Yes
10_03	Security	Acknowledgment and Reporting	Seven Years	Yes
09_01	Engineer	Applicability Assessment, Testing	Five Years	Yes
09_02	Network Administrator	Installation, Reporting	One Year	No
16_01	Test and Integration	Acknowledgment, Testing	Three Years	Yes
16_02	Network Administrator	Installation, Reporting	Six Months	No
NCC_01	Information Protection	Acknowledgment and Reporting of all base level TCNO compliance stats	Five Months	Yes
NOSC_01	Change Requests	Oversee TCNO compliance Reporting for the entire MAJCOM	Six Months	Yes
NOSC_02	Compliance Tracking	TCNO compliance tracking and reporting for entire MAJCOM	Two Years	Yes

One interesting item identified in the above table is that four of the interviewees were not familiar with the Air Force Regulation governing the TCNO process.

Results

The information gathered from all twelve interviewees was organized via "word tables" to enable data comparison and analysis. For the purposes of analysis, the data was grouped according to sub-research question topics and the interviewee data was grouped according to organization within each word table. A key point to remember when examining the interview data is that it is presented from an interviewee point of view and not the result of an analysis of quantitative, historical data. It is important to gather such information to ascertain whether those directly involved with the processes believe they are successfully meeting any and all predefined criteria set by existing policies or instructions such as those found in AFI 33-138 and to then compare those responses from actual historical data to see whether they align. Although written policies and procedures were requested from interviewee participants when relevant, none would accommodate this request as the interviewees felt providing this information would violate organizational policies.

Distribution

Table 7: TCNO Distribution

PMO Interviewee Results—TCNO Distribution		
Organization	**Distribution Methods**	**Process Description**
05	Email	The interviewee receives duplicate emails from two different sources—a parent organizational unit and the TCNO-D
10	Email, VMS	The security office receives notice of a TCNO in the form of an IAVA from the Vulnerability Management System; the testing office receives an email from the security office and the individual responsible for installation receives duplicate emails from the security office as well as the PMO
09	Email, Web	The testing entity is notified via email from the TCNO-D, but also uses an organizational website as information often appears earlier; In addition, the installation entity receives notification that the TCNO has been tested and approved from the PMO website; however installation is not authorized until the email sent from the NOSC is received which, according to the interviewee, is often several days later. The installation entity must manually acquire the installation instructions and software patch from two separate websites using two separate sets of credentials.
16	Email, Web	The testing entity is notified via email from the TCNO-D but also uses the AFCERT website since information tends to be posted a day or two prior. Once tested, the respective NOSCS receive an email. The NOSC sends an email to the base NCC Information Protection Office who forwards it to the appropriate installation entity. The entity responsible for installation receives an automated email from the PMO authorizing installation, however, implementation cannot occur until installation is not authorized until the email sent from the NOSC to the NCC and from the NCC to the Functional System Administrator responsible for implementation
NCC	Email, Action Tracker	The NCC information protection office receives the majority of its notifications via a SIPRNet application known as Action Tracker. This system is updated by the NOSC and contains information regarding all TCNOs applicable to NOSC and base-level assets. This data used for site selection in this research effort was extracted directly from Action Tracker. In addition, TCNO notification is supplemented by email from certain PMOs (as discussed above)
NOSC	Email, Action Tracker	The NOSC receives notifications for the PMOs it monitors via email; it then distributes TCNO notification to base level NCCs via Action Tracker and for certain PMOs via email (as discussed above)

The principal method of distribution used amongst all organizations studied was email, although this was often supplemented with other methods due to inherent inefficiencies in the process. For example, interviewees from PMO organizations 9 and 10 noted the fact that the email notifications they receive often lag a day or more behind the posting of the TCNO notification to the PMO's organizational website. They therefore check the websites regularly in order to get a head-start on subsequent processes such as applicability assessment and testing. One of the other issues gleaned from the interviewees, is that in the case of PMOs 9 and 16, neither can have TCNOs loaded until the NCC receives an authorization email from the NOSC even though the

PMO has already tested and approved installation on its systems. This introduces an obvious delay in the overall process time, often amounting to days or weeks of additional lag time according to interviewee accounts.

Even those that receive TCNO notification solely via email report shortcomings in the process. For example, the interviewee from PMO 5 expressed the fact that duplicate emails come from the TCNO-D site as well as from a parent organizational unit.

The process of distribution actually includes two main components—distribution of TCNO notification and distribution of the actual software patch. More often than not, these components are combined into one step, with the software patch attached or linked to the TCNO notification email. However in the case of organization 9, the two components are kept separate. Once the installation authority receives the TCNO notification and authorization to load, the Functional System Administrator (FSA) for organization 16 must go to two separate websites—one for the installation instructions and the other for the patch itself—both of which require separate login credentials.

Of the individuals interviewed that have oversight of TCNO distribution from the PMO level, three felt their respective processes met or exceeded the mandated timelines. The interviewee with this level of oversight for PMO 9 felt their overall process leading up to and including distribution has improved greatly, but that TCNOs “sometimes are sent out on the actual compliance date” and therefore automatically overdue.

Acknowledgment

Table 8: TCNO Acknowledgment

PMO Interviewee Results—TCNO Acknowledgment		
Organization	**Acknowledgment Methods**	**Process Description**
05	Email	Must acknowledge to both parent organizational unit and TCNO dashboard
10	VMS, TCNO-D	The security office acknowledges the IAVA through VMS, the testing entity acknowledges the TCNO through the TCNO-D
09	Email, TCNO-D	PMO testing entity acknowledges receipt through the TCNO-D; the NCC acknowledges receipt to the NOSC (see below) before passing the TCNO to the implementation authority
16	Email, TCNO-D	PMO testing entity acknowledges receipt through the TCNO-D; the NCC acknowledges receipt to the NOSC (see below) before passing the TCNO to the implementation authority
NCC	Action Tracker	NCC Information Protection office acknowledges receipt of all TCNOs to the NOSC via Action tracker
NOSC	Action Tracker	NOSC acknowledges receipt to the AFNOSC

A process required by the Air Force and one that is directly linked with distribution is that of TCNO acknowledgment. Once a process owner receives a TCNO through the distribution channels, they are required to formally acknowledge receipt back through the distribution chain. Since this process is so closely related to distribution, it appears, through the data gathered from this interview process, to be directly impacted by some of the previously mentioned shortfalls of the distribution process as well as have some of its own inherent weaknesses. For example, recall that PMO 5 receives TCNO notification from two sources—a parent organizational unit and the TCNO-D website. As a result, the interviewee involved in the process must also acknowledge the TCNO to both sources, an obvious duplication of effort.

Applicability Assessment

Table 9: TCNO Applicability Assessment

PMO Interviewee Results—TCNO Applicability Assessment		
Organization	**Applicability Assessment Methods**	**Timeline Allocated to Process**
05	Determined by Software/Operating System loaded	Within 24 hours
10	Determined by Software/Operating System loaded	Within 24 hours
09	Determined by Software/Operating System loaded	Within 24 hours
16	Determined by Software/Operating System loaded	Within 24 hours
NCC	Not Applicable (Performed by PMO)	-
NOSC	Not Applicable (Performed by PMO)	-

For all PMOs studied, the process of applicability assessment consists of comparing the software applications affected by the TCNO to the software or Operating System loaded on the applicable PMO assets. As a result, the timeframe allocated to this process did not vary considerably, with all PMOs completing this step of the process within 24 hours.

Testing

Table 10: TCNO Testing

PMO Interviewee Results—TCNO Testing					
Organization	**Testing Methods**	**Process Description**	**# Testing Facilities**	**Timeframe Allocated to Testing**	**Timeline Frequently Met?**
05	Server Login	The FSA loads the patch on the operational server and logs in to ensure it is still operational	1	Minutes to Hours--Testing performed immediately after TCNO implementation and lasts only as long as it takes to log in to the server and conduct a brief functionality check	Yes
10	Live testing lab	The TCNO is loaded in a live testing environment and operationally tested by a group of testers	1	30 days maximum depending upon TCNO	Yes
09	3 step process	The TCNO patch is tested as it is written; it is then sent to a lab environment to verify the written procedures; it is then sent to a third location for a final implementation test	3	Dependent upon classification of the TCNO and complexity of the TCNO fix action	Has improved. TCNO is sometimes distributed on the designated compliance date.
16	Functionality and peer review testing	Since TCNOs for this particular PMO also affect third-party controlled assets, the TCNO must be tested by this third party prior to implementation. Simultaneously, it is sent to a separate test and integration office where it undergoes basic functionality testing and a peer review process. This test and integration office will receive notification from the third party testing site once it has completed its testing process after which the TCNO can be released for implementation.	2 (both simultaneous)	14 days including holidays and weekends	Yes
NCC	Not Applicable (Performed by PMO)	-	-	-	-
NOSC	Not Applicable (Performed by PMO)	-	-	-	-

One important aspect to reiterate regarding the data in the above table is that it is based upon interviewee response, not verified historical data. Therefore, whether or not an organization frequently meets its own internal testing suspense timelines was not verified and instead was recorded based upon on the integrity and knowledge of the respondent. The interviewee from PMO 9 was the only one to convey delays in the testing process. While this interviewee could not specify as to where the delays might stem from specifically, based on the data in the table above, it may be due to the number of different testing entities involved coupled with the sequential nature of the testing process. Additionally, PMO 9 was also the only organization that could not provide a concrete timeline for the testing process. The interviewee only stated that the testing timeline was dependent upon multiple factors including the TCNO classification as well as the complexity of the fix action. The remaining three PMOs each had a definite timeframe associated with testing which was not to be exceeded regardless of the TCNO classification or fix action involved. One anomaly exhibited by PMO 5 is the order in which testing is performed—that is, after implementation. Although this PMO has only a handful of assets, testing in an operational environment after implementation goes against best practice recommendations. While it may save time, service interruptions realized by this order of process steps could ultimately prove far more detrimental than any time saved.

Implementation/Installation

Table 11: TCNO Installation

PMO Interviewee Results—TCNO Installation				
Organization	**Automated?**	**Process Description**	**Internal Timeframe Allocated to TCNO installation**	**Timeline Frequently Met?**
05	No	Log on to each asset directly, download the patch and load the patch manually	No—dictated by TCNO	Yes
10	No	Obtain patch from security office; log on to each asset remotely and manually load the patch	45 days	Yes
09	No	Log on to PMO website to obtain installation instructions; Log on to a second PMO website to download installation file; Log on to each asset remotely and run the TCNO installation file	No—dictated by TCNO	Generally meet the NOSC deadline but miss the PMO deadline
16	No	Obtain installation file directly from TCNO email notification; Log on to each asset remotely and run the TCNO installation file	No—dictated by TCNO	Yes
NCC	No	Some NCC personnel act as PMO FSAs	No—dictated by TCNO	Yes
NOSC	Partially	Some NOSC personnel act as PMO FSAs	-	Yes (For NOSC controlled PMO assets)

A problem that resurfaces in the installation process stems from the distribution methods utilized by the PMO TCNO process. For example, since the functional system administrator (FSA) for PMO 9 or PMO 16 cannot install the TCNO fix actions prior to receiving authorization from the NOSC and subsequently the NCC to which it reports, even if it has received PMO authorization, the timeline is often delayed. In the case of PMO 9, when the PMO releases authorization to load, it provides its own compliance suspense for the FSA to meet, which is generally no more than one to two weeks after release. Often, the NOSC authorization to load is released on or after this PMO suspense, which results in a failure to meet the compliance deadline before implementation can even begin. The cause for this time lag could not be determined through the interviews conducted. The FSA for PMO 16 as well as the NCC interviewee were both under the impression that additional testing was conducted at the NOSC level and this was the reason for the delay between PMO authorization to load and NOSC authorization to load.

However, when questioned about this, the testing authority from the PMO could not explain the lag time, stating that no such testing should occur at the NOSC level since it did not have the proper testing environment nor did it have a cause to test more extensively than was already being done by the PMO itself.

This raises another issue—which compliance deadline is authoritative from an FSA perspective? From those interviewed for this research, the only timeline that they are held accountable to is that which is imposed by the NOSC and subsequently tracked and enforced by the NCC. Again from an NCC's perspective, the NOSC directed compliance deadline is the one to which they are held accountable. However, at a higher level, the PMO itself is held accountable to meeting its own compliance deadline, which is why it makes an effort to test and distribute patches in a timely manner and subsequently generates its own compliance deadlines.

An additional consideration regarding implementation compliance timeframes is requesting extensions when necessary. Two of the interviewees did not know what procedures to follow if an extension request was necessary, while the rest all had a process in place to do so if required. However, one interviewee from PMO 9 admitted that it was not common practice to request extensions even when the compliance deadline was known to be missed. Instead, the organization allowed the status of the TCNO to become overdue without action.

The NOSC also acknowledged the fact that some of its TCNO installations are accomplished via automated means, but since this capability has not been instituted at the base level, the NCCs are forced to install the same TCNO software patches manually.

Reporting

Table 12: TCNO Reporting

PMO Interviewee Results—TCNO Reporting		
Organization	**Reporting Method**	**Process Description**
05	Email, Web	Report compliance to organizational parent unit and via TCNO-D
10	Email, VMS	The security office reports compliance of the IAVA through VMS; the PMO installation authority reports compliance both to the PMO organization and to the security office
09	Email	From a PMO perspective, compliance reporting is synonymous with acknowledgment—once it acknowledges via the TCNO-D it considers itself compliant. From an Air Force perspective, the PMO implementation authority reports compliance to the NCC which reports compliance to the NOSC
16	Action Tracker	The PMO implementation authority reports compliance to the NCC which reports compliance to the NOSC
NCC	Action Tracker	The NCC Information Protection Office reports TCNO compliance to the NOSC via Action Tracker
NOSC	Action Tracker	Reports compliance to the AFNOSC

Again, the communications channels of the reporting process practically mirror those of the distribution and acknowledgement processes. One source of conflicting opinion amongst a few of the interviewees stemmed from what constituted compliance and how compliance was reported. Perhaps one of the contributors to this confusion is the TCNO-D website itself. The website has a number of display options, one of which lists TCNOs in one column and their respective statuses in another, arranged by PMO. The status itself is conveyed via a "stoplight chart", with different colors signifying different status levels. Descriptions of each status level as they appear on the TCNO-D website are listed in table 13 below:

Table 13: TCNO-D Status Levels

TCNO-D Status Levels	
Status	**Description**
Green	Indicates that the TCNO can be Implemented
Yellow	Indicates that the TCNO has been Approved With Provisions
Blue	Indicates the PMO is still analyzing the effects of a TCNO for a specific system
Orange	Indicates the PMO has not stated any status as of yet and has not yet begun analysis
Grey	Indicates the TCNO for this PMO System does not apply and is not to be implemented
Red	Indicates that a color-coded light was originally Blue or Orange and is past due

This table illustrates that a "Green" status indicates the TCNO ***can*** be implemented, not that it has been implemented. Therefore, the TCNO-D is designed to enable TCNO acknowledgment, ***not*** compliance reporting. That being said, two PMOs use the website for this very purpose. The interviewee from PMO 5 uses the TCNO-D to acknowledge the TCNO and then waits to change the "Stoplight" status to Green until after successful implementation. At the other end of the spectrum, the interviewee from PMO 9 views TCNO acknowledgement and reporting as one in the same. Following testing and approval to implement from the PMO, the interviewee responsible for this process changes their respective PMO's status to Green on the TCNO-D site and at this point considers the PMO compliant with the TCNO. To the contrary, since no implementation has taken place at this point in time, the vulnerability has not been mitigated. That being said, the actual compliance (stemming from patch implementation) is tracked and recorded through Air Force channels since the assets for this PMO reside at a base level. Consequently, implementation status is reported from the implementation authority to the NCC and then to the NOSC and AFNOSC. These varying views of what constitutes compliance could however, cause great disparity in the historical compliance records maintained by the PMO and the Air Force.

The NCCs and the NOSC utilize two primary tools for compliance reporting--Action Tracker and Microsoft Systems Management Server (SMS). Action Tracker is a web-based tool that NCCs and NOSCs use to communicate the status of a TCNO. It uses a color-coded "stoplight" status reporting scheme similar to that of the TCNO-D discussed previously. While this tool provides the means to centralize compliance

reporting and monitoring, it is also completely manual, requiring technicians at each end to update the information on a regular basis. Both the NCC and the NOSC also use SMS which provides automatic TCNO compliance status updates (among other information) on a regular basis. For this process to be effective, each asset must have an SMS client loaded so that it can report its status back to a centralized server. Since these status updates are not real-time, there is some lag between the time an asset is patched with a TCNO fix action and the time it is reported to SMS. According to the interviewees at the NOSC, SMS is used as a verification tool to compare against the compliance data that are manually reported via Action Tracker.

Enforcing Compliance

The organizations with the primary responsibility of enforcing compliance are the NCC and their parent organization, the NOSC since it is these organizations that have oversight of the assets that reside on their respective networks. The interviewee with the responsibility to enforce compliance at the NCC level had both the authority and the ability to place noncompliant assets in a "quarantined" state until said assets were compliant or had a valid extension approved through the proper channels. They further stated that such quarantine actions have been taken in the past when deemed necessary and have proved effective. On the other hand, while two of the NOSC interviewees acknowledged the organization has both the authority and the ability to enforce compliance by removing any noncompliant asset from the network, to their knowledge, this had never been executed, even in times of asset non-compliance.

Accurate system inventory

When it came to controlling system accountability, each PMO maintained an inventory of which assets it controlled and where they were dispersed. In addition, the interviewee at the NCC knew how many assets it monitored and maintained a list of each PMO that resided at its location. The NOSC on the other hand, did not maintain such information. While it could provide a count of the systems it monitored via SMS, the interviewee responsible for NOSC TCNO compliance reporting could not provide a list of PMOs that reside on the NOSCs distributed network and for which TCNO compliance was mandated. The interviewee stated that the only way to determine such information would be to call each of the individual bases to collect the data.

V. Conclusions and Recommendations

Overview

This chapter is intended to answer the research questions, sub-questions and propositions developed and outlined in Chapters I and II by presenting the researcher's conclusions based on the results discussed in the previous chapter. This chapter is then concluded with limitations of the research as well as recommendations for future research.

Answers to Research Questions

RQ1). How does the lack of standardized, centrally managed, and enforced TCNO patching procedures for PMO impact the TCNO compliance timeframe and in turn, the security posture of the Air Force Network?

Each organization studied has implemented its own TCNO processes and methods of execution—some appear to work well, while others have significant negative impact on the TCNO compliance timeframe. Having a standardized, centrally managed and enforced TCNO patching process could exploit those methods that work well and enable all organizations to benefit from them. This is not to say that every TCNO process should be centrally controlled nor every method of TCNO process execution micromanaged. For example, forcing specific methods of testing on each PMO may beyond the scope of Air Force authority and such action would likely provide little process improvement; however, requiring minimum standards and enforcing timelines is essential to ensuring timely TCNO compliance. On the other hand, some TCNO

processes may benefit greatly from centralized control. For example instituting a standardized means of distribution, acknowledgment, reporting, monitoring, and overall means of communication could greatly decrease the amount of unnecessary work, streamline the TCNO process and significantly reduce the overall TCNO compliance timeline. To adequately do so requires centralized oversight and an awareness of the PMO asset landscape, which was not apparent during the course of this research. Each organization involved appears to only have a localized viewpoint of the TCNO processes and associated responsibilities. Also, not all processes appeared to have significant impact on the TCNO compliance timeframe. This is further illustrated by the results discussed in Chapter IV as well as the answers to the sub-research questions that appear below.

SRQ1). How do the methods of TCNO distribution (both to and from the PMOs) impact the TCNO compliance timeframe?

Amongst the four PMOs studied, no two distribution processes were identical, nor was there any distribution process without some imperfections. Each of the four organizations studied had at least one organization that was directly involved in the distribution process unnecessarily causing duplicate TCNO notifications, which again resulted in the requirement of redundant acknowledgment and compliance reporting. What set the high-performing PMOs apart from the low-performing PMOs was the fact that in the case of former, the overall implementation process did not rely on these extraneous organizations for TCNO implementation. In other words, in the instances

where there were multiple distribution channels, regardless of which source the TCNO was received, the next step in the process could occur immediately. Effectively, although there might have been multiple channels feeding it, the distribution process upon which the PMO relied to implement a TCNO for highest-performing organizations occurred as a single, logical process flow. On the other hand, the distribution process for low-performing organizations branches off and includes other Air Force organizational units, thereby adding additional steps in the process. For an illustration, refer to figure 3, a modification of the TCNO distribution process as outlined in AFI 33-138. In the case of the highest-performing PMOs, the process follows the dotted-line, where the PMO (or PMO designated organizational unit) distributes the PMO directly to the parties responsible for each of the subsequent steps (applicability assessment, testing, etc) and finally to the individual responsible for implementation. In the case of the low-performing PMOs, the process followed this same progression; however, there was a secondary process that occurred in tandem in which the PMO distributed its TCNO information to the NOSC which then distributed it to the NCC which then distributed it to the implementation authority. Although this secondary distribution process always took longer, it was also this process that the low-performing PMOs relied upon for TCNO implementation.

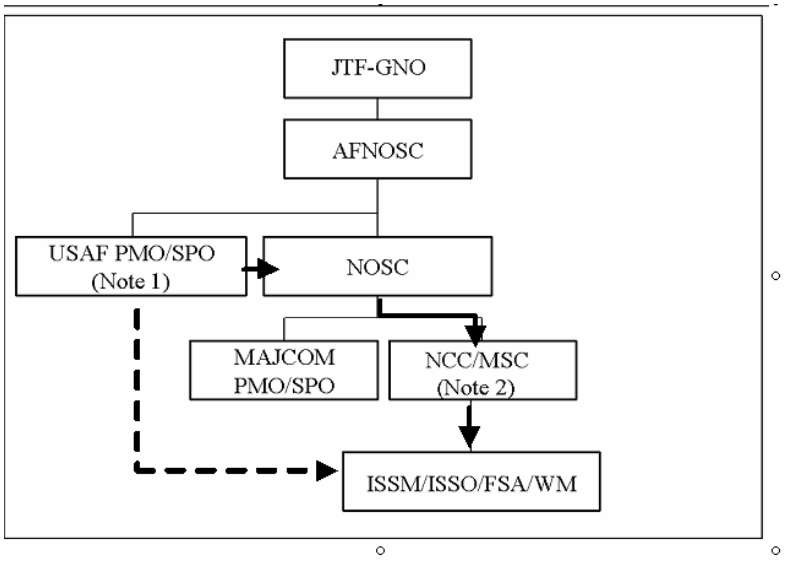


Figure 3: Apparent TCNO distribution process

Since the distribution process dictates not only how the organizational units involved in the TCNO process receives the TCNO information and fix actions but also how acknowledgment, compliance reporting and all other communications are conducted, adding additional steps to this process unnecessarily can have a profound effect on the compliance timeframe.

The other issue that warrants attention is the methods used for this process. While all organizations used email as a means of distribution, it was the way in which these emails were generated differed (ie automated vs. manual). The distribution method that appeared to work the best amongst those PMOs studied was the use of the TCNO dashboard (TCNO-D). This web-based system sent an automated email to all necessary process owners when a TCNO was listed on the website. It also provided a centralized means of acknowledgment and progress monitoring. Although both of the low-

performing PMOs utilized the TCNO-D for initial TCNO distribution and acknowledgment, the secondary distribution channel addressed earlier instituted additional distribution methods, none of which had the ability to interface with the TCNO-D and all of which were manually driven.

Again, the method of distribution tended to dictate all further lines of communication including TCNO acknowledgement and compliance reporting. Adding additional, stove-piped or manual methods appeared to further complicate these processes and as a result, lengthen the overall compliance timeline.

The distribution process must be streamlined so that only those organizations with a legitimate reason are involved in the TCNO distribution process. While it may be beneficial to provide some of these extraneous organizations the ability to monitor TCNO progress, making this oversight an additional, sequential (as opposed to concurrent) step in the distribution process does not add any value to the process and instead inhibits the timely implementation of the TCNO. In addition, there should be a single distribution method that utilizes automation as much as possible. This not only eliminates redundant processes and provides a single source of reference for process owners, but also reduces workload by reducing manual data entry.

SRQ2). How do PMO applicability assessment methods impact the TCNO compliance timeframe?

It does not appear that the applicability assessment process impacts the TCNO compliance timeframe a great deal as the process itself was straightforward and did not

vary considerably amongst the PMO organizations. In addition, for each of the PMOs studied, this process took minimal time and resources. The key to successfully assessing the applicability of a TCNO in a timely manner is an awareness of exactly what software is present on all applicable systems, which each PMO appeared to have.

SRQ3). How do PMO testing methods impact the TCNO compliance timeframe?

The testing process tended to vary considerably between the PMO organizations, with no apparent connection between the methods used and the compliance timeframe itself.

Recall from Chapter II that an ideal testing environment should "mimic the production environment as close as possible" (Voldal, 2003) and a successful testing process should ensure the patch: "corrects the vulnerability, does not open an old vulnerability, does not introduce a new vulnerability, does not degrade system performance and is compatible with all other required applications" (Grigg & Oleksak, 2004). PMO 10, one of the highest-performing organizations, satisfied both of these criteria by utilizing a live testing environment to mimic an operational environment. In addition, the distribution channels involved in this process were simplified by testing in one physical location and there was a definitive timeline associated with each TCNO testing period. On the other hand, PMO 9 utilized a three-step process with three separate physical locations, which introduced multiple lines of communication. There was also no apparent timeline that could be assigned with this process. The PMO with

the best testing timeline had it by default, since it performed no testing prior to TCNO implementation.

It appears, aside from not testing at all, a practice certainly not recommended by any professional literature reviewed for this study, implementing a thorough testing process in one physical location that mimics the production environment as closely as possible and follows a clear, enforced timeline has the least negative impact to the overall TCNO process. Again, while requiring all PMO organizations to follow the exact same testing procedures may be impractical, certain standards and oversight should apply to this process to reduce delays

SRQ4). How do PMO patching methods impact the TCNO compliance timeframe?

For all PMOs studied, a common weakness in the TCNO process was the fact that all patching is done manually. That being said, for many PMO organizations, a manual patching process was not implemented out of preference. In fact, an interviewee from PMO 9 expressed an organizational goal to develop or utilize an automated patching process such as SMS, but stated a lack of resources and manpower needed for the development of such a capability as the reason it has not come to fruition as of yet. The NOSC also expressed a desire for automated patching methods for all PMOs. One NOSC interviewee stated the lack of an automated means of patching PMO machines as a direct weakness to network security due to the additional time added to the patching process. Inherent in a manual patching process is an extended timeframe for implementation due to the work involved, the lack of centralized control and the obvious

limitations imposed by the number of patches one individual can install at any given time. On the other hand, automated tools such as SMS can install TCNO patches on thousands of machines simultaneously and "re-advertise" the installation of these patches on 24 hour timeline for any machines for which installation was not initially successful.

Interestingly, much of the lag time associated with TCNO patching stemmed not solely from the patching methods used but also from the point at which the implementation authority (ie FSA) was authorized to load the patch. Once again this goes back to the original means of distribution and the communication channels used in the overall TCNO process.

While it may not be possible to automate patching in the sense that all PMOs use the exact same method or tool, some form of automation should be a priority or even a requirement for each PMO that resides on the Air Force Network. That way, when a patch is authorized to load, installation can be centrally managed and performed in timely manner. In addition, there should be one and only one authority to approve implementation. FSAs for PMOs 9 and 16 expressed frustration with the fact that although the PMO authorized installation of the patch, they were not authorized to do so until after the NOSC released its own authorization, even though it appears there is no value added to the process (such as necessary additional testing) by the NOSC. Having more than one approval authority adds unnecessary time to the TCNO compliance timeframe.

SRQ5). How do PMO reporting methods impact the TCNO compliance timeframe?

Again, at the risk of being repetitive, the communications channels initially established by the distribution process also dictate the reporting channels and due to weaknesses already identified, there is much redundancy and a number of unnecessary steps involved in this process. This extends the TCNO compliance timeframe unnecessarily.

Compliance reporting (whether PMO or not), to a large degree, is done via manual means. This is supplemented to some extend by an automated tool (SMS), but the authoritative reporting data is manually entered into a web-based system which takes time and like any manual means, is subject to human error.

Also, as identified in Chapter IV, there was some confusion as to what constituted compliance reporting. Some organizations felt that acknowledgment of receipt was synonymous with compliance even though no patching had actually occurred. Although the TCNO-D is used by many PMOs, it does include the ability to report compliance statistics, a significant weakness.

Since all PMO assets on the NOSC controlled network are required to have SMS clients loaded as a means of observation, there appears to be little reason why compliance reporting cannot be done via automated means. In fact, interviewees at the NOSC expressed a desire to have TCNO compliance data for all machines on the network reported via an automated tool.

SRQ6). Are there any additional organizational behavior issues that might impact the TCNO compliance timeframe?

This research question was designed to highlight any additional organizational behavior issues that might be identified through the research process that would suggest an impact on the TCNO compliance timeframe. One of the issues identified was the organizational willingness to enforce TCNO compliance. In the case of the NCC, the approval authority had in fact enforced compliance by removing non-compliant PMO assets from operation. The NOSC, on the other hand, expressed a reluctance to take such action, even though they had the authority and ability. This goes beyond the TCNO process itself and instead points to a potential cultural impact on the compliance timeframe.

Answers to Propositions

Proposition 1: High-performing organizations have an accurate system inventory

This proposition proved accurate to a degree. All PMO organizations appeared to have an accurate picture of where their respective assets resided. Therefore, both well- and low-performing PMOs appeared to have accurate system inventories. However, the NOSC did not have a list of PMO assets that reside at each individual base under its control. While this did not have a direct impact on the four PMO TCNO compliance timeframes studied for this research effort, it is certainly a factor that could impact other PMO compliance timeframes. For example, during the interview process an NCC interviewee reported an additional 8 PMOs that existed at the base level that the NOSC was not aware of. While the NOSC may not (and possibly should not) be directly

involved in the TCNO patching process for those PMOs, a failure to maintain an accurate system inventory results in a failure to maintain awareness of resulting network vulnerabilities.

Proposition 2: Despite a possible similarity in TCNO compliance results, due to the lack of standardized TCNO processes, the methods of process execution will vary amongst all PMO organizations studied.

This proposition proved to be accurate as outlined in the results section of Chapter IV and further highlighted above in the answers to the research questions. No two organizations had exactly the same TCNO processes.

Proposition 3: There will be noticeable difference in the TCNO processes (or the execution of those processes) of high-performing and low-performing PMO organizations

The proposition also proved to be accurate. Perhaps the overwhelming difference between well and low-performing organizations was the communications channels used for the execution of the TCNO processes. This appeared to have much to do with how dispersed the PMO organizations were and as a result, which organizations they had to interact with. Therefore, other similarities in organizational characteristics may contribute to process execution such as geographic disbursement of assets and organizational size.

Limitations

The results of this study may not be generalized across the entire Air Force. The four PMOs studied cannot account for all processes and methods of execution used by every PMO across the Air Force. In the case of identifying best practices, there may be organizations that have implemented procedures that would greatly benefit the development of a standardized Air Force TCNO process for PMOs. While the historical data used for site selection was analyzed largely by automated means, there was some degree of manual data input on the part of the researcher. Therefore there is the possibility of an incorrect or erroneous entry. That being said, since site selection was based upon several factors and five years of historical data a small number of input errors should have little impact on the end result. This historical data was also originally gathered via a system (Action Tracker) that relies on manual data entry. Therefore, human error may have been introduced at this point as well. Since no direct observation was used in this study, aside from site selection the results were based upon interviewee self-reporting. The interview process and resulting data analysis may be impacted by research bias since both were conducted by the same individual.

Recommendations for Action and Future Research

One thing this research identified was that the PMO TCNO process (as well as the overall Air Force TCNO process) needs one, centralized means for communication. This includes TCNO distribution, acknowledgement, reporting and monitoring. Having disparate, disconnected systems operating at multiple levels provides limited oversight of

the overall security posture of the Air Force network and negatively impacts the TCNO compliance timeframe. Also, the extent of manual work involved in the existing systems also impacted the compliance timeframe and potentially influenced compliance data. Perhaps the largest obstacle encountered during initial data collection for site selection was the lack of standardization in the data itself. Often a PMO's name would appear in the database under several different name variations. One PMO had over 40 different variations of its name appear in the database. This makes it very difficult to accurately capture historical data for a given organization without running the risk of omitting potentially important data. A great deal of information would need to be gathered from all entities involved including PMOs and impacted Air Force organizations in order to develop a solution to these problems. Further research should be conducted to either develop a new system that would correct existing problems or further develop an existing system such as the TCNO-D so that it might meet all of these needs.

There are likely additional organizational factors both physical and behavioral that influence the TCNO process. Factors such as organizational size or levels of autonomy provided to those involved in the process could impact the overall TCNO compliance timeframe. Size in particular was a factor common to like-performing organizations, with the two low-performing organizations being amongst the largest and the two best-performing organizations being amongst the smallest. Although, the two lowest-performing organizations utilized almost the exact same communications channels for the majority of their processes, which appeared to be a major inhibiting factor, size may well have an impact of its own. It seems likely that the fewer assets an organization

has, the easier it should be to manage them. Further research could examine how organizational size impacts the TCNO process and if it is indeed an obstacle, how to overcome it. Also research could be conducted to examine a PMO organization, possible through direct observation, to determine what, if any, organizational behavior issues impact the TCNO process and to what degree.

Conclusion

This research was intended to examine the existing TCNO processes used by PMOs and interacting Air Force agencies to identify potential shortfalls and ultimately provide recommendations for improvement in an effort to move towards a standardized TCNO patching process. It is evident that there is currently no means of quickly and accurately identifying all PMOs or PMO assets that reside on the Air Force Network, a problem that requires attention in order to truly understand the existing vulnerabilities to this network's security posture.

By interviewing those involved in these processes, it is also apparent that there are no standardized methods of execution for TCNO processes used by PMO organizations and that these processes would likely benefit from a standardized, centrally managed and enforced approach. While not all TCNO procedures appear to impact the TCNO compliance timeframe equally, there are some that deserve greater attention. Specifically, a standardized means of distribution, acknowledgment, reporting, monitoring, and overall means of communication could greatly decrease the amount of unnecessary work, streamline the TCNO process, and significantly reduce the overall TCNO compliance timeline.

Appendix A: Case Study Protocol and Case Study Database Format

Overview of the Case Study

Background

Network security is a paramount concern for organizations utilizing computer technology, and the Air Force is no exception. The Air Force deploys network security patches as Time Compliance Network Orders (TCNOs), which together with associated processes and enforced timelines ensure network compliance. The current AF method to track and manage the TCNO process amongst its many PMOs is extremely limited and fragmented at best. There is no current or planned, standardized method to release TCNOs to PMOs within the AF. In order to improve existing PMO patch management methods, we must examine the entire process including patch distribution, assessment, testing, patching and reporting practices used by PMOs operating within the bounds of the Air Force network. Consequently, this study will examine how the lack of standardized, centrally managed, and enforced TCNO patching procedures for PMO impact the TCNO compliance timeframe and in turn, the security posture of the Air Force Network.

Key documents

- The Air Force Regulation that governs the TCNO process is AFI 33-138
- Pending Air Force Guidance: Vulnerability Lifecycle Management System (VLMS) Concept of Operations (CONOPS)
- Previous Air Force thesis research: Kubinsky (2004) Securing the Air Force Network: Issues Concerning Time Compliance Network Order Deployment

Sponsorship

This research is being sponsored by 8th AF, DET 1/AFNOSC.

Contact: Capt Mario Oliver
Assistant Director of Operations
DSN: 312.781.7235
CML: 318.456.7235
Mario.Oliver@BARKSDALE.AF.MIL

Field Procedures

To set up an interview

Start with an email (see format below) to establish contact and explain the purpose of the interview. Follow up with a phone call.

[Rank] [Name],

My name is Lt Mike Czumak. I am a student at the Air Force Institute of Technology conducting research regarding Air Force Time Compliance Network Orders (TCNOs). Specifically, the goal of this research is to gain a better understanding of how Project Management Offices with assets operating on the Air Force Network perform the TCNO process and from this understanding, develop potential recommendations for standardized processes, process improvements and identify any best practices.

I understand you are involved with this process for your organization and I would like to conduct an interview to gather data for my research. Please contact me at michael.czumak@afit.edu if you are able to participate and we can set up a time convenient for you.

If you have any questions, please don't hesitate to contact me. I have also included my thesis advisor's contact information below:

> Thesis Advisor: Dr. Michael Grimaila – Phone 937-255-3636 (DSN 785) x. 4800; E-mail – michael.grimaila@afit.edu.

Thanks,

Michael Czumak III, 1Lt, USAF
Student, Air Force Institute of Technology (AFIT)
School of Engineering and Management (ENV)
MS Information Resource Management (GIR-07S) Information Assurance and Strategic Management Sequences
michael.czumak@afit.edu

Immediately prior to the interview:

- Review pertinent information
- Ensure to have the following information readily available:
  - Air Force Regulations governing TCNOs
  - Any correspondence previously made with the interviewee
  - List of Questions/Question Answer Sheet
  - Laptop for recording answers
  - Voice Recorder

At the start of the interview:

1. Researcher Introduction: “My name is Lt Mike Czumak. I am a student at the Air Force Institute of Technology conducting Air Force (8AF/AFNOSC) sponsored research regarding Air Force Time Compliance Network Orders (TCNOs).”

2. Read the purpose statement: “The goal of this research is to gain a better understanding of how Project Management Offices with assets operating on the Air Force Network perform the TCNO process and from this understanding, develop potential recommendations for standardized processes, process improvements and identify any best practices.”

3. Describe the interview process: “This will be a semi-structured interview. I have a short list of questions, which may lead to additional questions for further research or clarification purposes. Please feel free to interject any information you feel may be useful to the research.”

4. Assure anonymity: “I want to remind you that no identifying information obtained through this or subsequent interviews will be retained or reported in the final research report. In order to complete the research effort, data collected on individual subjects may include general duty description of/duration in current position, but no names (of interviewee or organization) or position identifiers will be retained. Data gathering will be focused on information specific to Air Force and PMO TCNO procedures.”

5. Record interviewee information and interview start time on record sheet

6. Ask the appropriate questions, depending on the interviewee (see below)

Following the Interview:

- Record interview stop time on record sheet

- Consolidate all information into Case Study Database (see attached)

- Follow up with an email which should contain the following elements (see template below):
    - Short message thanking the participant for their time
    - Request for any outstanding information necessary for completing the report
    - Full contact information of researcher and thesis advisor
    - Reiteration of any information promised to the interviewee during the interview

> [Rank] [Name],
>
> Thank you for participating in the [telephone] interview conducted on [date]. The information you provided will certainly contribute to my research efforts.
>
> As discussed, I would appreciate your assistance in obtaining the following documents: [As applicable]
>
> Also, as discussed, I owe you the following information/deliverables: [As applicable]
>
> In addition, you will receive a copy of the draft thesis for your review prior to publishing.
>
> If you have any questions, please don't hesitate to contact me.
>
> Thanks again,
>
> Michael Czumak III, 1Lt, USAF
> Student, Air Force Institute of Technology (AFIT)
> School of Engineering and Management (ENV)
> MS Information Resource Management (GIR-07S) Information Assurance and Strategic Management Sequences
> michael.czumak@afit.edu

A Guide for the Study Report

The final case study report will be written in the approved Air Force Institute of Technology thesis format.

Attachments:
1) Case Study Questions
2) Case Study Database Format

Case Study Questions

The interviews of this case study are designed to be semi-structured. The questions listed below are tailored to the intended interviewee. These questions are meant to provide a direction, focus and general flow of the interview; however, other lines of questioning are likely to develop based on interviewee responses. For interview data collection, copy the appropriate questions onto designated section of the Interview Data Collection Sheet, which appears later in this Attachment following the Case Study Database Format. Each interview will have its own Interview Data Collection Sheet. Any additional questions that may come up during the interview and their respective answers must also be recorded in the same manner.

Although the majority of interviews conducted in this research study are intended to be conducted via telephone and with the answers recorded by the researcher, the questions listed below are presented in a format that allows for them to be sent and responded to via email should the need arise. If this is the case, an introduction and directions are provided at the end of this section to be included with the questions.

Project Management Office Interview Outline **SECTION 1: INTERVIEWEE INFO**	
Question 1:	Please provide your general job description (please <u>do not</u> include a specific duty title or position identifier):
Answer:	*Please write your answer in this space*
Question 2:	Please describe your role in your PMO's TCNO process.
Answer:	
Question 3:	How long have you been working with the Air Force TCNO process? (Years/Months):
Answer:	
Question 4:	How many assets are you personally responsible for ensuring TCNO compliance?
Answer:	
Question 5:	Are you familiar the Air Force TCNO-D (Dashboard) website? Do you utilize it?
Answer:	
Question 6:	Are you familiar with the Air Force regulation governing TCNO procedures?
Answer:	
****If you answered "Yes" to the above question, continue to Question 6a.**	

If you answered "No", please proceed to Section 2: Organizational/PMO Info.	
Question 6a:	To what capacity, if any does your PMO use the regulation in its TCNO processes?
Answer:	
SECTION 2: ORGANIZATIONAL/PMO INFO	
Question 1:	What function do your PMO assets (that reside on the Air Force network) perform?
Answer:	
Question 2:	How many assets does your PMO currently have operating on the Air Force network? Has this number changed significantly in the past 5 years?
Answer:	
Question 3:	How many people are assigned to the Air Force TCNO process in your PMO?
Answer:	
Question 4:	Do you maintain other assets besides those that reside on the Air Force network?
Answer:	
****If you answered "Yes" to the above question, continue to Question 4a. If you answered "No", please proceed to Section 3: Organizational/PMO Procedures.**	
Question 4a:	Is the security patching of these assets managed by separate guidance?
Answer:	
Question 4b:	Do you feel that guidance is more or less effective? Why?
Answer:	
SECTION 3: ORGANIZATIONAL/PMO PROCEDURES	
Question 1:	Does your PMO have written policies/procedures regarding TCNO compliance for your assets that reside on the Air Force network?
Answer:	
****If you answered "Yes" to the above question, continue to Question 1a. If you answered "No", please proceed to the Question 2.**	
Question 1a:	Do these policies/procedures differ in any way from the security patching procedures that apply to other PMO assets not residing on the AF network (if applicable)?
Answer:	

Question 1b:	When were these policies/procedures created?	
Answer:		
Question 1c:	When were these policies/procedures last updated?	
Answer:		
Question 1d:	By whom are these policies/procedures maintained?	
Answer:		
Question 2:	Do you have established written procedures for the following five situations? (Please write 'Yes' or 'No' in the provided spaces)	
Answer:	The TCNO does not apply to the program	
	The TCNO applies to the program and the FSAs are authorized to implement the countermeasure according to the procedures contained in the TCNO.	
	The TCNO applies to the program but the FSAs are not authorized to implement the countermeasure according to the procedures contained in the TCNO.	
	The TCNO applies to the program but actual implementation procedures are not yet available.	
	The applicability of the TCNO to the program is not known at this time.	
Question 3:	How (email, hard copy, website) and from whom do you receive notice of Air Force TCNOs?	
Answer:		
Question 4:	Are you responsible for TCNO **acknowledgment**?	
Answer:		
****If you answered "Yes" to the above question, continue to Question 4a. If you answered "No", please proceed to the Question 4d.**		
Question 4a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.	
Answer:		
Question 4b:	Is this process followed for every TCNO?	
Answer:		
Question 4c:	What is the timeframe allocated to this process?	

Answer:	
Question 4d *(only answer if you answered "No" to question 4):*	Who is responsible for this process? Can you provide their contact information?
Answer:	
Question 5:	Are you responsible for determining TCNO **applicability** on your systems? (Applicability indicates whether the TCNO will be installed on at least one of your PMO systems residing on the Air Force Network)
Answer:	
****If you answered "Yes" to the above question, continue to Question 5a. If you answered "No", please proceed to the Question 5d.**	
Question 5a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 5b:	Is this process followed for every TCNO?
Answer:	
Question 5c:	What is the timeframe allocated to this process?
Answer:	
Question 5d *(only answer if you answered "No" to question 5)*:	Who is responsible for this process? Can you provide their contact information?
Answer:	
Question 6:	Are you responsible for TCNO **testing** on your systems?
Answer:	
****If you answered "Yes" to the above question, continue to Question 5a. If you answered "No", please proceed to the Question 5e.**	
Question 6a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 6b:	Is this process followed for every TCNO?

Answer:	
Question 6c:	What is the timeframe allocated to this process?
Answer:	
Question 6d:	Is this process conducted in one location/facility?
Answer:	
Question 6e *(only answer if you answered "No" to question 6):*	Who is responsible for this process? Can you provide their contact information?
Answer:	
Question 7:	Are you responsible for TCNO **installation** on your systems?
Answer:	
****If you answered "Yes" to the above question, continue to Question 7a. If you answered "No", please proceed to the Question 7d.**	
Question 7a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 7b:	Is this process followed for every TCNO?
Answer:	
Question 7c:	What is the timeframe allocated to this process?
Answer:	
Question 7d *(only answer if you answered "No" to question 7):*	Who is responsible for the installation process (ie. base level FSAs, another organization, etc.)? May I have their contact information?
Answer:	
Question 8:	Are you responsible for **reporting** TCNO compliance?
Answer:	
****If you answered "Yes" to the above question, continue to Question 8a. If you answered "No", please proceed to the Question 8e.**	

Question 8a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 8b:	Is this process followed for every TCNO? If not, list any exceptions.
Answer:	
Question 8c:	What is the timeframe allocated to this process?
Answer:	
Question 8e *(only answer if you answered "No" to question 7):*	Who is responsible for the reporting process (ie. base level FSAs, another organization, etc.)? May I have their contact information?
Answer:	
Question 9:	Do you maintain historical records of your TCNO compliance?
Answer:	
Question 10:	Is there an overall set timeline/deadline allocated to the TCNO process for your PMO? Is this timeline frequently met? If not, how much would you say it is exceeded on average?
Answer:	
Question 10a:	By whom and how is this timeline determined?
Answer:	
Question 10b:	Is this timeline frequently met? If not, how much would you say it is exceeded on average?
Answer:	
Question 11:	What procedures do you follow if you require an extension for a given TCNO?
Answer:	
Question 11a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 12:	Are there any other organizations you interface with to ensure TCNO compliance? (Please list)

Answer:	
Question 13:	Do you utilize any automated methods in your TCNO patching process? If not, are there any procedure you would like to see automated (please explain)?
Answer:	
Question 14:	Are there any methods of TCNO process management (to include any processes used to ensure TCNO compliance) used within your PMO that you feel work particularly well?
Answer:	
Question 15:	Do you have any general comments or recommendations for improvement to the overall TCNO patching/management process?
Answer:	
Question 16:	May I receive an electronic copy of any TCNO written procedures your PMO maintains? (If so, please attach it to your email response.) If you do not maintain any written guidance, is there an individual I may speak with to better understand the processes you employ?
Answer:	

MAJCOM NOSC Interview Outline (MAJCOM PMO-Specific Contacts) SECTION 1: INTERVIEWEE INFO	
Question 1:	Please provide your general job description (please do not include a specific duty title or position identifier):
Answer:	*Please write your answer in this space*
Question 2:	Please describe your role in your PMO's TCNO process.
Answer:	
Question 3:	How long have you been working with the Air Force TCNO process? (Years/Months):
Answer:	
Question 4:	How many assets are you personally responsible for ensuring TCNO compliance?
Answer:	
Question 5:	Are you familiar the Air Force TCNO-D (Dashboard) website? Do you utilize it?
Answer:	
Question 6:	Are you familiar with the Air Force regulation governing TCNO procedures?
Answer:	
****If you answered "Yes" to the above question, continue to Question 6a. If you answered "No", please proceed to Section 2: Organizational/PMO Info.**	
Question 6a:	To what capacity, if any does your PMO use the regulation in its TCNO processes?
Answer:	
SECTION 2: ORGANIZATIONAL/PMO INFO	
Question 1:	What function do your PMO assets (that reside on the Air Force network) perform?
Answer:	
Question 2:	How many assets does your PMO currently have operating on the Air Force network within your MAJCOM? Has this number changed significantly in the past 5 years?
Answer:	
Question 3:	How many people are assigned to the Air Force TCNO process for your PMO at your MAJCOM?

Answer:		
Question 4:	Do you maintain other assets besides those that reside on the Air Force network?	
Answer:		
****If you answered "Yes" to the above question, continue to Question 4a. If you answered "No", please proceed to Section 3: Organizational/PMO Procedures.**		
Question 4a:	Is the security patching of these assets managed by separate guidance?	
Answer:		
Question 4b:	Do you feel that guidance is more or less effective? Why?	
Answer:		
SECTION 3: ORGANIZATIONAL/PMO PROCEDURES		
Question 1:	Does the PMO have written policies/procedures regarding TCNO compliance for your assets that reside on the Air Force network?	
Answer:		
****If you answered "Yes" to the above question, continue to Question 1a. If you answered "No", please proceed to the Question 2.**		
Question 1a:	Do these policies/procedures differ in any way from the security patching procedures that apply to other PMO assets not residing on the AF network (if applicable)?	
Answer:		
Question 1b:	When were these policies/procedures created?	
Answer:		
Question 1c:	When were these policies/procedures last updated?	
Answer:		
Question 1d:	By whom are these policies/procedures maintained?	
Answer:		
Question 2:	Do you have established written procedures for the following five situations? (Please write 'Yes' or 'No' in the provided spaces)	
Answer:	The TCNO does not apply to the program	

	The TCNO applies to the program and the FSAs are authorized to implement the countermeasure according to the procedures contained in the TCNO.	
	The TCNO applies to the program but the FSAs are not authorized to implement the countermeasure according to the procedures contained in the TCNO.	
	The TCNO applies to the program but actual implementation procedures are not yet available.	
	The applicability of the TCNO to the program is not known at this time.	
Question 3:	How (email, hard copy, website) and from whom do you receive notice of Air Force TCNOs?	
Answer:		
Question 4:	Are you responsible for TCNO **acknowledgment**?	
Answer:		
****If you answered "Yes" to the above question, continue to Question 4a. If you answered "No", please proceed to the Question 4d.**		
Question 4a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.	
Answer:		
Question 4b:	Is this process followed for every TCNO?	
Answer:		
Question 4c:	What is the timeframe allocated to this process?	
Answer:		
Question 4d *(only answer if you answered "No" to question 4):*:	Who is responsible for this process? Can you provide their contact information?	
Answer:		
Question 5:	Do you determine TCNO **applicability** on your systems or is this done by another entity? (Applicability indicates whether the TCNO will be installed on at least one of your PMO systems residing on the Air Force Network)	
Answer:		

****If you answered "Yes" to the above question, continue to Question 5a. If you answered "No", please proceed to the Question 6.**	
Question 5a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 5b:	Is this process followed for every TCNO?
Answer:	
Question 5c:	What is the timeframe allocated to this process?
Answer:	
Question 6:	Do you perform TCNO **testing** on your systems or is this performed by another entity?
Answer:	
****If you answered "Yes" to the above question, continue to Question 6a. If you answered "No", please proceed to the Question 7.**	
Question 6a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 6b:	Is this process followed for every TCNO?
Answer:	
Question 6c:	What is the timeframe allocated to this process?
Answer:	
Question 6d:	Is this process conducted in one location/facility?
Answer:	
Question 7:	Are you responsible for TCNO **installation** on your systems?
Answer:	
****If you answered "Yes" to the above question, continue to Question 7a. If you answered "No", please proceed to the Question 7d.**	
Question 7a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	

Question 7b:	Is this process followed for every TCNO?
Answer:	
Question 7c:	What is the timeframe allocated to this process?
Answer:	
Question 7d *(only answer if you answered "No" to question 6):*	Who is responsible for the installation process (ie. base level FSAs, another organization, etc.)? May I have their contact information?
Answer:	
Question 8:	Are you responsible for **reporting** TCNO compliance?
Answer:	
****If you answered "Yes" to the above question, continue to Question 8a. If you answered "No", please proceed to the Question 8e.**	
Question 8a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 8b:	Is this process followed for every TCNO? If not, list any exceptions.
Answer:	
Question 8c:	What is the timeframe allocated to this process?
Answer:	
Question 8e *(only answer if you answered "No" to question 7):*	Who is responsible for the reporting process (ie. base level FSAs, another organization, etc.)? May I have their contact information?
Answer:	
Question 9:	Do you maintain historical records of your TCNO compliance?
Answer:	
Question 10:	Is there an overall set timeline/deadline allocated to the TCNO process for your PMO? Is this timeline frequently met? If not, how much would you say it is exceeded on average?

Answer:	
Question 10a:	By whom and how is this timeline determined?
Answer:	
Question 10b:	Is this timeline frequently met? If not, how much would you say it is exceeded on average?
Answer:	
Question 11:	What procedures do you follow if you require an extension for a given TCNO?
Answer:	
Question 11a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 12:	Are there any other organizations you interface with to ensure TCNO compliance? (Please list)
Answer:	
Question 13:	Do you utilize any automated methods in your TCNO patching process? If not, are there any procedure you would like to see automated (please explain)?
Answer:	
Question 14:	Are there any methods of TCNO process management (to include any processes used to ensure TCNO compliance) used within your PMO that you feel work particularly well?
Answer:	
Question 15:	Do you have any general comments or recommendations for improvement to the overall TCNO patching/management process?
Answer:	
Question 16:	May I receive an electronic copy of any TCNO written procedures your PMO maintains? (If so, please attach it to your email response.) If you do not maintain any written guidance, is there an individual I may speak with to better understand the processes you employ?
Answer:	

MAJCOM CONTACTS RESPOSIBLE FOR GENERAL TCNO PROCEDURES SECTION 1: INTERVIEWEE INFO	
Question 1:	Please provide your general job description (please do not include a specific duty title or position identifier):
Answer:	*Please write your answer in this space*
Question 2:	Please describe your role in your MAJCOM's TCNO process.
Answer:	
Question 3:	How long have you been working with the Air Force TCNO process? (Years/Months):
Answer:	
Question 4:	How many assets are you personally responsible for ensuring TCNO compliance?
Answer:	
Question 5:	Are you familiar the Air Force TCNO-D (Dashboard) website? Do you utilize it?
Answer:	
Question 6:	Are you familiar with the Air Force regulation governing TCNO procedures?
Answer:	
****If you answered "Yes" to the above question, continue to Question 6a. If you answered "No", please proceed to Section 2: PMO Asset Info.**	
Question 6a:	To what capacity, if any does your PMO use the regulation in its TCNO processes?
Answer:	
SECTION 2: PMO ASSET INFO	
Question 1:	How many PMOs reside in the MAJCOM?
Answer:	
Question 2:	How many PMO assets reside in the MAJCOM?
Answer:	
Question 3:	How many of these PMOs/assets reside at the MAJCOM level (report directly to the MAJCOM NOSC)?
Answer:	
Question 4:	How many of these PMOs/assets reside at the base NCC level (report directly to the base NCC)? In these cases, who oversees TCNO compliance?

Answer:	
SECTION 3: ORGANIZATIONAL PROCEDURES	
Question 1:	What guidance do you follow that dictates the TCNO process for your MAJCOM?
Answer:	
Question 2:	Is there an established method for identifying all PMO machines in your MAJCOM?
Answer:	
Question 3:	Do you have the ability to scan/remotely monitor PMO machines for security vulnerabilities?
Answer:	
Question 4:	How and from whom do you receive notice that a TCNO is due for a PMO asset?
Answer:	
Question 5:	How do you communicate with FSAs responsible for PMO assets under your area of responsibility?
Answer:	
Question 6:	Does anyone at the MAJCOM level act as an FSA for any PMO assets?
Answer:	
Question 7:	How are you notified of TCNO compliance?
Answer:	
Question 8:	Are you responsible for reporting PMO TCNO compliance status?
Answer:	
****If you answered "Yes" to the above question, continue to Question 8a. If you answered "No", please proceed to Question 9.**	
Question 8a:	To whom do you report compliance?
Answer:	
Question 8b:	What procedures do you use and who dictates these procedures?

Answer:	
Question 9:	How are you notified of a PMO TCNO extension request and what is the process for validating this request?
Answer:	
Question 10:	Do you enforce PMO asset compliance if there is no valid extension? How?
Answer:	
Question 11:	Do you have the ability and authority to quarantine PMO machines that do not comply with TCNO policies?
Answer:	
****If you answered "Yes" to the above question, continue to Question 11a. If you answered "No", please proceed to Question 12.**	
Question 11a:	Do you have any PMO assets that are not exempt from automated TCNO patching? Which ones?
Answer:	
Question 12:	Are there any other organizations you interface with to ensure TCNO compliance? (Please list)
Answer:	
Question 13:	Do you utilize any automated methods in your TCNO patching process? If not, are there any procedure you would like to see automated (please explain)?
Answer:	
Question 14:	Do you audit/oversee individual PMO TCNO procedures such as testing, applicability assessment, installation, etc?
Answer:	
Question 15:	Are there any methods of TCNO process management (to include any processes used to ensure TCNO compliance) used within your PMO that you feel work particularly well?
Answer:	
Question 16:	Do you have any general comments or recommendations for improvement to the overall TCNO patching/management process?
Answer:	

Question 17:	May I receive an electronic copy of any TCNO written procedures your PMO maintains? (If so, please attach it to your email response.) If you do not maintain any written guidance, is there an individual I may speak with to better understand the processes you employ?
Answer:	

BASE-LEVEL NCC CONTACTS RESPOSIBLE FOR GENERAL TCNO PROCEDURES SECTION 1: INTERVIEWEE INFO	
Question 1:	Please provide your general job description (please do not include a specific duty title or position identifier):
Answer:	*Please write your answer in this space*
Question 2:	Please describe your role in your Base's TCNO process.
Answer:	
Question 3:	How long have you been working with the Air Force TCNO process? (Years/Months):
Answer:	
Question 4:	How many assets are you personally responsible for ensuring TCNO compliance?
Answer:	
Question 5:	Are you familiar the Air Force TCNO-D (Dashboard) website? Do you utilize it?
Answer:	
Question 6:	Are you familiar with the Air Force regulation governing TCNO procedures?
Answer:	
****If you answered "Yes" to the above question, continue to Question 6a. If you answered "No", please proceed to Section 2: PMO Asset Info.**	
Question 6a:	To what capacity, if any does your PMO use the regulation in its TCNO processes?
Answer:	
SECTION 2: PMO ASSET INFO	
Question 1:	How many PMOs reside at your base?
Answer:	
Question 2:	How many total PMO assets reside at your base?
Answer:	
SECTION 3: ORGANIZATIONAL PROCEDURES	
Question 1:	What guidance do you follow that dictates the TCNO process for your base (specifically for PMOs)?
Answer:	

Question 2:	Is there an established method for identifying all PMO machines at your base?
Answer:	
Question 3:	Do you have the ability to scan/remotely monitor PMO machines for security vulnerabilities?
Answer:	
Question 4:	How and from whom do you receive notice that a TCNO is due for a PMO asset?
Answer:	
Question 5:	How do you communicate with FSAs responsible for PMO assets under your area of responsibility?
Answer:	
Question 6:	Does anyone at the base NCC level act as an FSA for any PMO assets?
Answer:	
Question 7:	How are you notified of PMO TCNO compliance?
Answer:	
Question 8:	Are you responsible for reporting PMO TCNO compliance status?
Answer:	
****If you answered "Yes" to the above question, continue to Question 8a. If you answered "No", please proceed to Question 9.**	
Question 8a:	To whom do you report PMO compliance?
Answer:	
Question 8b:	What procedures do you use and who dictates these procedures?
Answer:	
Question 9:	How are you notified of a PMO TCNO extension request and what is the process for validating this request?
Answer:	
Question 10:	Do you enforce PMO asset compliance if there is no valid extension? How?
Answer:	

Question 11:	Do you have the ability and authority to quarantine PMO machines that do not comply with TCNO policies?
Answer:	
****If you answered "Yes" to the above question, continue to Question 11a. If you answered "No", please proceed to Question 12.**	
Question 11a:	Do you have any PMO assets that are not exempt from automated TCNO patching? Which ones?
Answer:	
Question 12:	Are there any other organizations you interface with to ensure PMO TCNO compliance? (Please list)
Answer:	
Question 13:	Do you utilize any automated methods in your PMO TCNO patching process? If not, are there any procedure you would like to see automated (please explain)?
Answer:	
Question 14:	Do you audit/oversee individual PMO TCNO procedures such as testing, applicability assessment, installation, etc?
Answer:	
Question 15:	Are there any methods of TCNO process management (to include any processes used to ensure TCNO compliance) used within your PMO that you feel work particularly well?
Answer:	
Question 16:	Do you have any general comments or recommendations for improvement to the overall TCNO patching/management process?
Answer:	
Question 17:	May I receive an electronic copy of any TCNO written procedures your PMO maintains? (If so, please attach it to your email response.) If you do not maintain any written guidance, is there an individual I may speak with to better understand the processes you employ?
Answer:	

FSA Interview Outline SECTION 1: INTERVIEWEE INFO	
Question 1:	Please provide your general job description (please do not include a specific duty title or position identifier):
Answer:	*Please write your answer in this space*
Question 2:	Please describe your role in the TCNO process.
Answer:	
Question 3:	How long have you been working with the Air Force TCNO process? (Years/Months):
Answer:	
Question 4:	How many assets are you personally responsible for ensuring TCNO compliance?
Answer:	
Question 5:	For how many different PMOs are you responsible for ensuring TCNO compliance?
Answer:	
Question 6:	Are you familiar the Air Force TCNO-D (Dashboard) website? Do you utilize it?
Answer:	
Question 7:	Are you familiar with the Air Force regulation governing TCNO procedures?
Answer:	
****If you answered "Yes" to the above question, continue to Question 7a. If you answered "No", please proceed to Section 2: Organizational/PMO Info.**	
Question 7a:	To what capacity, if any does your PMO use the regulation in its TCNO processes?
Answer:	
SECTION 2: ORGANIZATIONAL/FSA PROCEDURES	
Question 1:	Is there separate guidance you are required to follow for each PMO?
Answer:	
****If you answered "Yes" to the above question, continue to Question 1a. If you answered "No", please proceed to the Question 2.**	
Question 1a:	Do you feel that any of this guidance is more or less effective than others? Why?

Answer:	
Question 1b:	When were these policies/procedures created?
Answer:	
Question 1c:	When were these policies/procedures last updated?
Answer:	
Question 1d:	By whom are these policies/procedures maintained?
Answer:	
Question 2:	How (email, hard copy, website) and from whom do you receive notice of Air Force TCNOs?
Answer:	
Question 3:	Are you responsible for TCNO **acknowledgment**?
Answer:	
****If you answered "Yes" to the above question, continue to Question 3a. If you answered "No", please proceed to the Question 3d.**	
Question 3a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 3b:	Is this process followed for every TCNO?
Answer:	
Question 3c:	What is the timeframe allocated to this process?
Answer:	
Question 3d *(only answer if you answered "No" to question 4):*:	Who is responsible for this process? Can you provide their contact information?
Answer:	
Question 4:	Do you determine TCNO **applicability** on your systems or is this done by another entity? (Applicability indicates whether the TCNO will be installed on at least one of your PMO systems residing on the Air Force Network)

Answer:	
****If you answered "Yes" to the above question, continue to Question 4a. If you answered "No", please proceed to the Question 5.**	
Question 4a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 4b:	Is this process followed for every TCNO?
Answer:	
Question 4c:	What is the timeframe allocated to this process?
Answer:	
Question 5:	Do you perform TCNO **testing** on your systems or is this performed by another entity?
Answer:	
****If you answered "Yes" to the above question, continue to Question 5a. If you answered "No", please proceed to the Question 6.**	
Question 5a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 5b:	Is this process followed for every TCNO?
Answer:	
Question 5c:	What is the timeframe allocated to this process?
Answer:	
Question 5d:	Is this process conducted in one location/facility?
Answer:	
Question 6:	Are you responsible for TCNO **installation** on your systems?
Answer:	
****If you answered "Yes" to the above question, continue to Question 6a. If you answered "No", please proceed to the Question 6d.**	
Question 6a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.

Answer:	
Question 6b:	Is this process followed for every TCNO?
Answer:	
Question 6c:	What is the timeframe allocated to this process?
Answer:	
Question 6d *(only answer if you answered "No" to question 6):*	Who is responsible for the installation process (ie. Another base level entity, another organization, etc.)? May I have their contact information?
Answer:	
Question 7:	Are you responsible for **reporting** TCNO compliance?
Answer:	
****If you answered "Yes" to the above question, continue to Question 7a. If you answered "No", please proceed to the Question 7d.**	
Question 7a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 7b:	Is this process followed for every TCNO? If not, list any exceptions.
Answer:	
Question 7c:	What is the timeframe allocated to this process?
Answer:	
Question 7d *(only answer if you answered "No" to question 7):*	Who is responsible for the reporting process (ie. Another base level entity, another organization, etc.)? May I have their contact information?
Answer:	
Question 8:	Do you maintain historical records of your TCNO compliance?
Answer:	
Question 9:	Is there an overall set timeline/deadline allocated to the TCNO process for your PMO? Is this timeline frequently met? If not, how much would you say it is

	exceeded on average?
Answer:	
Question 9a:	By whom and how is this timeline determined?
Answer:	
Question 9b:	Is this timeline frequently met? If not, how much would you say it is exceeded on average?
Answer:	
Question 10:	What procedures do you follow if you require an extension for a given TCNO?
Answer:	
Question 10a:	Is this process dictated by established written guidance? If not, please describe the process in as much detail as possible.
Answer:	
Question 11:	How do you monitor compliance of your assets?
Answer:	
Question 12:	Are there any other organizations you interface with to ensure TCNO compliance? (Please list)
Answer:	
Question 13:	Do you utilize any automated methods in your TCNO patching process? If not, are there any procedure you would like to see automated (please explain)?
Answer:	
Question 14:	Are there any methods of TCNO process management (to include any processes used to ensure TCNO compliance) used within your PMO that you feel work particularly well?
Answer:	
Question 15:	Do you have any general comments or recommendations for improvement to the overall TCNO patching/management process?
Answer:	
Question 16:	May I receive an electronic copy of any TCNO written procedures your PMO maintains? (If so, please attach it to your email response.) If you do not maintain any written guidance, is there an individual I may speak with to better understand the processes you employ?
Answer:	

Interview Introduction (to be included with interviews that are conducted via email)

Thank you for participating in this sponsored Air Force Institute of Technology research project. The goal of this research is to gain a better understanding of how Project Management Offices with assets operating on the Air Force Network perform the TCNO process and from this understanding, develop potential recommendations for standardized processes and identify any best practices. If you have any questions about the questions themselves or any other aspect of the research, please don't hesitate to contact me at michael.czumak@afit.edu .

Please note: No identifying information obtained through this or subsequent interviews will be retained or reported in the final research report. In order to complete the research effort, data collected on individual subjects may include general duty description of/duration in current position, but no names (of interviewee or organization/PMO) or position identifiers will be retained. Data gathering will be focused on information specific to Air Force and PMO TCNO procedures.

Directions: Please answer the following questions to the best of your ability. There are answer spaces provided for each question as illustrated in the below example. Please feel free to add any space necessary to answer the questions. Some questions have multiple parts. Please answer the main question first, followed by any applicable sub-questions. Questions with multiple parts will have instructions guiding you along the way (denoted by a **):

Example (note the directions provided under the answer space denoted by a **):

Question 4:	Are you familiar with the Air Force regulation governing TCNO procedures?
Answer:	*Please write your answer in this space*
****If you answered "Yes" to the above question, continue to Question 4a. If you answered "No", please proceed to Section 2: Organizational/PMO Info.**	

Since this research is focused on how TCNO processes are conducted in PMO organizations, the final question requests copies of any PMO TCNO guidance/policy. If you are able to provide such guidance, please attach said guidance to your reply email. If you are not able to provide such guidance, please describe the process in as much detail as possible when requested in the question.

Again, thank you for participating in this research effort. Your inputs are highly valued and appreciated.

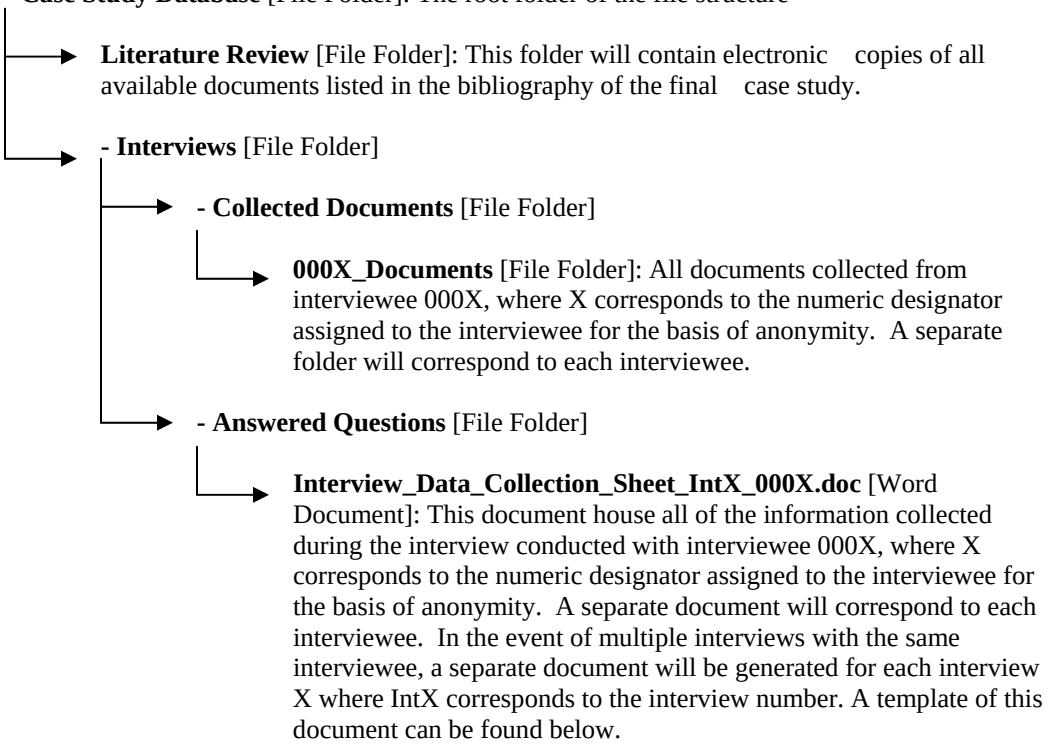
Very Respectfully,
Lt Michael Czumak
Student, Air Force Institute of Technology (AFIT)

Case Study Database Format

The case study database is designed to organize the data collected during the course of conducting this case study. It is comprised of a basic file structure and a few key documents.

File Structure

- **Case Study Database** [File Folder]: The root folder of the file structure



Literature Review [File Folder]: This folder will contain electronic copies of all available documents listed in the bibliography of the final case study.

- Interviews [File Folder]

- Collected Documents [File Folder]

000X_Documents [File Folder]: All documents collected from interviewee 000X, where X corresponds to the numeric designator assigned to the interviewee for the basis of anonymity. A separate folder will correspond to each interviewee.

- Answered Questions [File Folder]

Interview_Data_Collection_Sheet_IntX_000X.doc [Word Document]: This document house all of the information collected during the interview conducted with interviewee 000X, where X corresponds to the numeric designator assigned to the interviewee for the basis of anonymity. A separate document will correspond to each interviewee. In the event of multiple interviews with the same interviewee, a separate document will be generated for each interview X where IntX corresponds to the interview number. A template of this document can be found below.

Other Key Documents

A basic Microsoft Excel Spreadsheet titled **Interview_Info.xls** will link to the above file structure for consolidated access. The format of the spreadsheet is as follows:

Interviewee #	Organization Identifier	Interview Start Time	Interview End Time	Questions/Answers	Collected Documents
0001	PMO1			Click here	Click Here
0002	PMO2			Click here	Click Here
0003	PMO2			Click here	Click Here
0004	PMO3			Click here	Click here
0005	PMO3			Click here	Click here
0006	PMO4			Click here	Click here

As can be seen above, for each interviewee, there is a link to the corresponding **Interview_Data_Collection_Sheet_000X.doc** under the Questions/Answers column. In addition, there is a link to the corresponding **Collected Documents** file folder.

Location

The finalized case study database will be transferred to 2 CDs, one to be provided to the thesis advisor and the other to remain with the researcher.

Interview Data Collection Sheet (Template)

Interviewee #: 0001
Organization #: 0001
Date:
Interview Time:

Interview Questions and Answers

Question 1:
Answer 1:

•
•
•
•

Question N
Answer N

Additional Documents to be sent by Interviewee

Document Name/Description Promised Date

Additional Information to be provided to Interviewee by Researcher

Description Promised Date

Appendix B: Selection Criteria Data

Ranked Totals Based On Historical Data—Lowest Performers

This table is a list of all PMOs included in the final data analysis. Each PMO was ranked in each category based on the analysis of the historical performance data as outlined in Chapter 4 (with 1 being the poorest and 46 being the best). Each PMO's ranks were totaled and the list was ordered based on these totals. The top 25% in each category are highlighted. The last three columns contain descriptive data about each PMO.

	Network Security Impact			Performance Measures				Descriptive Data			
PMO	Most Non-Compliant Patches	Most Non-Compliant TCNOs	Most "Serious" or "Critical" Overdue/Non-Compliant TCNOs"	Most Days Overdue Per TCNO	Highest % Non Compliant TCNOs	Highest % Overdue TCNOs	Total	Highest Workoad (Most Total Patches)	Most Dispersed	Least Workload (total patches)	Least Dispersed
9	5	2	1	10	7	9	34	3	2	44	10
16	1	1	2	24	3	15	46	1	1	46	11
42	2	3	14	16	2	14	51	5	4	42	8
12	19	6	12	5	14	1	57	15	9	32	3
3	14	8	5	2	20	11	60	16	10	31	2
15	7	9	21	9	9	5	60	17	11	30	1
45	17	5	16	11	4	7	60	26	11	21	1
40	4	4	6	20	11	19	64	7	3	40	9
11	13	9	19	15	13	1	70	22	9	25	3
37	16	7	19	18	5	6	71	24	9	23	3
7	10	14	13	7	28	3	75	4	9	43	3
39	23	12	11	8	22	4	80	21	7	26	5
13	28	15	10	3	30	1	87	19	10	28	2
33	20	12	19	26	10	1	88	36	11	11	1
28	15	6	24	30	1	18	94	37	9	10	3
21	6	14	8	29	29	12	98	6	11	41	1
17	38	16	9	4	31	2	100	18	11	29	1
19	12	9	15	13	17	34	100	9	5	38	7
20	11	12	3	32	25	17	100	8	11	39	1
4	18	14	26	6	15	25	104	29	11	18	1
14	30	14	31	22	6	1	104	42	11	5	1
26	21	13	29	43	1	1	108	44	11	3	1
2	9	10	19	34	12	26	110	12	8	35	4
23	24	13	7	27	27	16	114	30	11	17	1
1	3	12	27	19	19	35	115	10	6	37	6
18	39	16	4	21	31	8	119	2	10	45	2
29	27	13	22	33	8	21	124	41	11	6	1
24	25	14	18	23	23	22	125	27	10	20	2
43	8	14	25	31	21	27	126	11	10	36	2
6	36	16	32	12	31	1	128	40	11	7	1
36	43	16	25	1	31	13	129	34	11	13	1
32	22	11	17	28	18	35	131	23	10	24	2
8	32	15	31	17	16	29	140	31	11	16	1
38	44	16	27	14	31	10	142	25	11	22	1
25	26	14	32	44	1	28	145	45	11	2	1
30	29	15	30	36	4	35	149	39	11	8	1
22	31	14	14	42	26	23	150	28	11	19	1
27	40	16	28	41	31	1	157	43	11	4	1
41	45	16	32	35	31	1	160	13	10	34	2
31	33	15	32	46	4	35	165	46	11	1	1
35	42	16	25	37	31	20	171	32	11	15	1
44	34	15	23	45	24	30	171	38	11	9	1
10	37	16	31	25	31	33	173	35	11	12	1
46	46	16	20	40	31	24	177	14	10	33	2
34	41	16	25	38	31	31	182	20	9	27	3
5	35	16	31	39	31	32	184	33	10	14	2

Ranked Totals Based On Historical Data—Highest Performers

This table is a list of all PMOs included in the final data analysis. Each PMO was ranked in each category based on the analysis of the historical performance data as outlined in Chapter 4 (with 1 being the best and 46 being the poorest). Each PMO's ranks were totaled and the list was ordered based on these totals. The top 25% in each category are highlighted. The last three columns contain descriptive data about each PMO.

	Network Security Impact			Performance Measures				Descriptive Data			
PMO	Least Non-Compliant Patches	Least Non-Compliant TCNOs	Least "Serious" or "Critical" Overdue/Non-Compliant TCNOs"	Least Days Overdue Per TCNO	Lowest % Non Compliant TCNOs	Lowest % Overdue TCNOs	Total	Highest Workoad (Most Total Patches)	Most Dispersed	Least Workload (total patches)	Least Dispersed
5	1	1	2	8	1	4	17	33	10	14	2
34	1	1	7	9	1	5	24	20	9	27	3
44	2	2	9	2	8	6	29	38	11	9	1
10	1	1	2	22	1	3	30	35	11	12	1
46	1	1	11	7	1	12	33	14	10	33	2
31	2	2	1	1	28	1	35	46	11	1	1
35	1	1	7	10	1	16	36	32	11	15	1
22	3	3	17	5	6	13	47	28	11	19	1
27	1	1	4	6	1	35	48	43	11	4	1
30	4	2	3	11	29	1	50	39	11	8	1
41	1	1	1	12	1	35	51	13	10	34	2
25	5	3	1	3	33	8	53	45	11	2	1
8	2	2	2	30	16	7	59	31	11	16	1
32	7	6	14	19	14	1	61	23	10	24	2
43	20	3	7	16	11	9	66	11	10	36	2
38	1	1	5	33	1	26	67	25	11	22	1
24	5	3	13	24	9	14	68	27	10	20	2
29	5	4	9	14	24	15	71	41	11	6	1
6	1	1	1	35	1	35	74	40	11	7	1
1	25	5	5	28	13	1	77	10	6	37	6
23	6	4	23	20	5	20	78	30	11	17	1
36	1	1	7	46	1	23	79	34	11	13	1
2	19	7	12	13	20	10	81	12	8	35	4
18	1	1	26	26	1	28	83	2	10	45	2
26	7	4	3	4	34	35	87	44	11	3	1
4	10	3	6	41	17	11	88	29	11	18	1
20	17	5	27	15	7	19	90	8	11	39	1
19	16	8	16	34	15	2	91	9	5	38	7
21	22	3	23	18	3	24	93	6	11	41	1
14	3	3	2	25	26	35	94	42	11	5	1
17	1	1	22	43	1	34	102	18	11	29	1
28	13	11	8	17	35	18	102	37	9	10	3
33	8	5	12	21	22	35	103	36	11	11	1
13	4	2	21	44	2	35	108	19	10	28	2
39	7	5	20	39	10	32	113	21	7	26	5
7	18	3	18	40	4	33	116	4	9	43	3
37	12	10	12	29	27	30	120	24	9	23	3
11	15	8	12	32	19	35	121	22	9	25	3
40	24	14	24	27	21	17	127	7	3	40	9
3	14	9	25	45	12	25	130	16	10	31	2
15	21	8	10	38	23	31	131	17	11	30	1
45	11	13	15	36	30	29	134	26	11	21	1
12	9	12	19	42	18	35	135	15	9	32	3
42	26	15	17	31	32	22	143	5	4	42	8
16	27	17	28	23	31	21	147	1	1	46	11
9	23	16	29	37	25	27	157	3	2	44	10

Rank-ordered top 25% of PMOs in each category with corresponding values

Most Non Compliant Patches	
PMO #	Value
16	1411
42	1163
1	1093
40	625
9	312
21	116
15	113
43	113
2	94
7	88
20	65

Most Non-Compliant TCNOs	
PMO #	Value
16	93
9	56
42	31
40	25

Most Overdue/ Non-Compliant TCNOs Serious or Critical	
PMO #	Value
9	89
16	70
20	59
18	56
3	53
40	49
23	46
21	46

Highest % Non-Compliant TCNOs	
PMO #	Value
28	100.00%
26	100.00%
25	100.00%
42	70.45%
16	62.84%
45	50.00%
30	50.00%
31	50.00%

Highest% Overdue TCNOs	
PMO #	Value
13	100.00%
12	100.00%
6	100.00%
11	100.00%
14	100.00%
33	100.00%
41	100.00%
27	100.00%
26	100.00%
17	98.55%
7	98.46%
39	98.04%
15	95.83%
37	95.65%

Most Days Overdue Per TCNO	
PMO #	Value
36	291.85
3	279.91
13	275.28
17	270.74
12	242.37
4	220.01
7	203.37
39	198.00
15	182.33
9	181.72

Most Dispersed (Number of Units)	
PMO #	Value
17	77
10	67
41	16

Highest Workload (Total Patches)	
PMO #	Value
16	27263
18	16410
9	10897
7	10791
42	7334
21	4103
40	3819
20	3679
19	2311
1	1981

Least Non Compliant Patches	
PMO #	Value
27	0
46	0
5	0
34	0
35	0
41	0
10	0
18	0
38	0
6	0
17	0
36	0
31	2
44	2
8	2
22	4
14	4
30	5
13	5
25	6
29	6
24	6
23	8
26	9
32	9
39	9

Least Non-Compliant TCNOs	
PMO #	Value
41	0
27	0
6	0
10	0
5	0
36	0
38	0
35	0
46	0
34	0
17	0
18	0
31	1
30	1
8	1
44	1
13	1
25	2
14	2
4	2
43	2
24	2
22	2
7	2
21	2
26	3
29	3
23	3
33	4
1	4
39	4
20	4

Least Overdue/ Non-Compliant TCNOs Serious or Critical	
PMO #	Value
41	0
6	0
31	0
25	0
10	1
5	1
8	1
14	1
30	2
26	2
27	3
38	4
1	4
4	5
36	6
35	6
34	6
43	6
28	7

Lowest % Non-Compliant TCNOs	
PMO #	Value
41	0.00%
27	0.00%
6	0.00%
10	0.00%
5	0.00%
36	0.00%
38	0.00%
35	0.00%
46	0.00%
34	0.00%
17	0.00%
18	0.00%
13	1.43%
21	3.03%
7	3.08%
23	4.00%
22	4.65%
20	4.71%
44	5.00%
24	5.88%

Lowest % Overdue TCNOs	
PMO #	Value
31	0.00%
30	0.00%
1	0.00%
32	0.00%
19	5.00%
10	16.67%
5	33.33%
34	34.78%
44	35.00%
8	40.00%
25	50.00%
43	64.00%

Least Days Overdue Per TCNO	
PMO #	Value
31	0.00
44	0.77
25	14.00
26	19.50
22	21.05
27	22.67
46	26.18
5	34.50
34	36.73
35	38.83

Least Dispersed (Number of Units)	
PMO #	Value
31	2
25	2
26	2
27	2
14	2
29	2
6	2
30	2
44	2
33	2
10	2
36	2
35	2
8	2
23	2
4	2
22	2
45	2
38	2
17	2
15	2
20	2
21	2
5	3
24	3
32	3
13	3
3	3
46	3
41	3
43	3
18	3
28	4
37	4
11	4
34	4
12	4
7	4

Lowest Workload (Total Patches)	
PMO #	Value
31	4
25	6
26	13
27	15
14	16
29	24
6	28
30	37
44	41
28	43

Action Tracker Database Tables used to mine historical data

PMO : Table

Field Name	Data Type
ATPID	Number
ATPUnitID	Number
ATPActionID	Number
ATPDate	Date/Time
ATPPMO	Text
ATPAffected	Number
ATPPatched	Number
ATPMAC	Number
ATPComment	Text
Patchable	Yes/No
Patchcomment	Text
PMOID	Number
SIPRAffected	Number
SIPRPatched	Number
Majcom	Text

actions : Table

Field Name	Data Type
ActionID	Number
ActionType	Text
ShortName	Text
AffectedSystem	Text
SuspenseDate	Date/Time
SuspenseNote	Text
Show	Text
Description	Memo
RelatedURL	Memo
Title	Text
AnnounceDate	Date/Time
AFNOSC	Text
Statistic	Text
DODID	Text
ReportToAF	Text
IAVA	Text
CITS2	Yes/No
CITS2_Patch	Yes/No
DMS2	Yes/No
DMS2_Patch	Yes/No
DMS3	Yes/No
DMS3_Patch	Yes/No
ReportTo	Text
ActionStatus	Text
ActionSubType	Text
CloseDate	Text
Classification	Text
ActionNeeded	Memo
Remarks	Memo
ReportProcedure	Memo
Impact	Text
ReceiptDate	Date/Time
StatsDate	Date/Time
IAVANumber	Text
SupercededBy	Text
Updated	Yes/No
MailSent	Yes/No
TempDate	Date/Time

SQL Queries used to mine data from database

PMOs with more than 1 affected asset

```
SELECT DISTINCT (pmo.atppmo)
FROM actions, pmo
WHERE actions.actiontype="TCNO" And pmo.atpactionID=actions.actionid And pmo.atpaffected>0
ORDER BY pmo.ATPPMO;
```

Number of Different TCNOs

```
SELECT count(*)
FROM [SELECT DISTINCT (actions.shortname)
FROM actions, pmo
WHERE actions.ActionType="TCNO" And pmo.ATPActionID=actions.actionid And
pmo.ATPAffected>0 And (pmo.ATPPMO=forms!form1.List_PMO_Names.value)
ORDER BY actions.ShortName]. AS [%$##@_Alias];
```

Number of Non-Compliant Patches

```
SELECT sum(pmo.atpaffected-pmo.atppatched) AS Expr1
FROM pmo, actions
WHERE actions.ActionType="TCNO" And pmo.ATPActionID=actions.actionid And
pmo.ATPAffected>0 And (pmo.atppatched<pmo.atpaffected) And (pmo.atpaffected-pmo.atppatched)>0
And (pmo.ATPPMO=forms!form1.List_PMO_Names.value);
```

Number Non-Compliant TCNOs

```
SELECT count(pmo.atpunitid) AS Expr1
FROM actions, pmo
WHERE (((actions.ActionType)="TCNO") And ((pmo.ATPActionID)=actions.actionid) And
((pmo.ATPAffected)>0) And ((pmo.ATPPMO)=forms!form1.List_PMO_Names.value)) And
pmo.atppatched<pmo.atpaffected;
```

Number of Units

```
SELECT count(*)
FROM [select  Distinct(pmo.atpunitid)
FROM actions, pmo
WHERE actions.ActionType="TCNO" And pmo.ATPActionID=actions.actionid And
pmo.ATPAffected>0 And pmo.ATPPMO=forms!form1.List_PMO_Names.value]. AS [%$##@_Alias];
```

Total Days Non-Compliant

```
SELECT sum(pmo.atpdate-actions.suspensedate) AS Expr1
FROM pmo, actions
WHERE actions.ActionType="TCNO" And pmo.ATPActionID=actions.actionid And
pmo.ATPAffected>0 And (pmo.atpdate>actions.suspensedate) And (pmo.atpaffected-pmo.atppatched)>0
And (pmo.ATPPMO=forms!form1.List_PMO_Names.value);
```

Appendix C: Human Subjects Exemption Approval

DEPARTMENT OF THE AIR FORCE
AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

22 November 2006

MEMORANDUM FOR AFIT/ENV (MICHAEL R GRIMAILA)

FROM: AFRL/Wright Site Institutional Review Board

SUBJECT: Request for exemption from human experimentation requirements

1. Protocol title: Development of a Standardized Time Compliance Network Order (TCNO) Patching Process.

2. Protocol number: F-WR-2007-0007-E

3. The above protocol has been reviewed by the AFRL Wright Site IRB and determined to be **exempt** from IRB oversight and human subject research requirements per 32 CFR 219.101(b)(2) which exempts "research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior."

4. This exemption applies only to the requirements of 32 CFR 219, DoDD 3216.2, AFI 40-402, and related human research subject regulations. If this project is a survey, attitude or opinion poll, questionnaire or interview, consult AFI 36-2601, Air Force Personnel Survey Program, for further guidance. Headquarters AFPC/DPSAS is the final approval authority for conducting attitude and opinion surveys within the Air Force.

5. The IRB must be notified if there is any change to the design or procedures of the research to be conducted. Otherwise, no further action is required.

6. For questions or concerns, please contact the IRB administrator, Helen Jennings at (937) 904-8094 or helen.jennings@wpafb.af.mil OR Lt. Douglas Grafel at douglas.grafel@wpafb.af.mil or (937) 656-5437. All inquiries and correspondence concerning this protocol should include the protocol number and name of the primary investigator.

JEFFREY BIDINGER, Maj, USAF, MC, FS
Chair, AFRL/Wright Site IRB

References

AFI 33-138. (2005). Air Force Instruction 33-138. Enterprise Network Operations Notification and Tracking

Alliegro, C. (2003). "Windows Patch Management: How Microsoft Patches its Own Client PCs [Electronic Version]. Directions on Microsoft. Retrieved July 12, 2006 from http://www.directionsonmicrosoft.com/sample/DOMIS/update/2004/01jan/0104cpam.htm

Barker, D. (2006). "A Good Patch Management Strategy". Inacom Information Systems. Retrieved October 14, 2006 from http://www.inacom.com/display.aspx?page=/newsletter/patch.aspx

Barney, D. (2005). "The 10 Essential Rules of Patch Management" *Redmond Mag*. Retrieved July 11, 2006 from http://redmondmag.com/features/article.asp?EditorialsID=459

Benbasat, I., Goldstein, D.K., Mead, M. (1987). "The Case Research Strategy in Studies of Information Systems". *MIS Quarterly*, Sep, 369-386.

Brandman, G. (2005). "Patching the Enterprise". *ACM Queue*, 3(2). ACM Press, 2005, pp 32-39.

CERT (2006). CERT/CC Statistics 1988-2006. Retrieved July 11, 2006 from http://www.cert.org/

Chan, J. (2004). "Essentials of Patch Management Policy and Practice". Patch Management.org. Retrieved July 12, 2006 from http://www.patchmanagement.org/pmessentials.asp

Chan, W. L. (2003). Patch Management--Best Practices: SANS Institute.

Colville, R., Wagner, R., Nicolett, M. (2002). "Patch Management Benefits, Challenges and Prerequisites". Gartner Research. Retrieved July 11, 2006 from http://www.appliednetsec.com/productresources/patchlink/patch%20management%20concerns.pdf

Cashell, B. Jackson W.D., Jickling, M., Webel, B. (2004). "The Economic Impact of Cyber Attacks: CRS Report for Congress". April 1 2004. Retrieved July 12 2006 from http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

Dadzie, J. (2005). "Understanding Software Patching". *ACM Queue*, 3(2). ACM Press, 2005, pp 24-31.

Dube, L., Pare, G. (2001). Case Research in Information Systems: Current Practices, Trends, and Recommendations. Retrieved September 18, 2006 from http://cat.inist.fr/?aModele=afficheN&cpsidt=14387515

GAO. (2003). “Effective Patch Management is Critical to Mitigating Software Vulnerabilities” (No. GAO-03-1138T): United States General Accounting Office.

GAO. (2003). “Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures” (No. GAO-03-564T): United States General Accounting Office.

GAO. (2004). Agencies Face Challenges in Implementing Effective Software Patch Management Processes (No. GAO-04-816T): United States General Accounting Office.

Statement by John Gilligan, Chief Information Officer, United States Air Force, Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities House Armed Service Committee United States House Of Representatives. (2003). Retrieved April 17, 2006 from http://www.globalsecurity.org/military/library/congress/2004_hr/04-03-31gilligan.htm

Kelvin, W.T.. (1883). "Electrical Units of Measurement", PLA, vol. 1. Available as of February 12, 2007 at http://zapatopi.net/kelvin/quotes/

Kubinsky (2004) “Securing the Air Force Network: Issues Concerning Time Compliance Network Order Deployment.” Thesis. Air Force Institute of Technology.

Leedy, P.D, Ormrod, J.E. (2005). Practical Research: Planning and Design 8th Edition. Prentice Hall. New Jersey.

Mell, P., Tracy, C. M. (2002). Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology (No. 800-40): National Inistitute of Standards and Technology.

Microsoft. (2004). “Patch Management Process”. Microsoft TechNetRetrieved March 6, 2006 from http://www.microsoft.com/technet/security/guidance/patchmanagement/secmod193.mspx

Nicastro, F. M. (2003). “Security Patch Management: High Level Overview of the Patch Management Process”. International Network Services. Retrieved April 6, 2006 from http://www.only4gurus.com/techlib/miscellaneous/ins_white_paper_security_patch_mgmt_0303.pdf

Oleksak, C. G. J. (2004). “IT Security--How Important is Patch Management?”. Universal Advisor(1). Retrieved July 11, 2006 from http://www.plantemoran.com/Publications/Universal+Advisor/2004+Issue+No+1/IT+Security+how+important+is+patch+management.htm

Perez, J.C. (2001). Gartner: Most IT security problems self-inflicted. IDG News Service

Qualls, M. (2004). “Possible Points of Failure in the Information Security Environment”. SANS Institute Whitepaper. Retrieved May 22, 2006 from http://www.sans.org/reading_room/whitepapers/infosec/1437.php

Roberge, C. (2004). “Patch Management Best Practices”. Cressida Technology Whitepaper. Retrieved July 11, 2006 from http://www.cressida.info/pdfs/whitepapers/bestpractices.pdf

Schouten, C.L. (2003). “Protecting Large Industrial Organisations from the new breed of Virus Attack”. SANS Institute Whitepaper. Retrieved May 22, 2006 from http://www.giac.org/certified_professionals/practicals/gsec/4003.php

Schwartz, M. (2004). “Solving the Patch Management Headache: Best practices in keepting the desktop secure”. *Enterprise Systems Journal.* Retrieved October 14, 2006 from http://esj.com/security/article.aspx?EditorialsID=852

Voldal, D. (2003). A Practical Methodology for Implementing a Patch Management Process: SANS Institute Whitepaper. Retrieved July 11, 2006 from http://www.giac.org/certified_professionals/practicals/gsec/3168.php

Wall, B. (2006, January 7). Fear Factor: Stocking up on security. International Herald Tribune, Retrieved July 11, 2006 from http://www.iht.com/articles/2006/01/27/yourmoney/msecure.php

Walther, J. (2004). “ Meeting the Challenges of Automated Patch Management”. SANS Institute Whitepaper. Retrieved July 11, 2006 from http://www.giac.org/certified_professionals/practicals/gsec/4024.php

Wrenn, G. (2004). “Welded Shut: How to Patch Vulnerabilities and Keep Them Sealed”. Information Security News, 22 Nov 2004. Retrieved July 11, 2006 from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1027338,00.html

Yin, K. (2003). *Case Study Research: Design and Methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
22-03-2007	**Master's Thesis**	Jun 2000 – Jul 2006

4. TITLE AND SUBTITLE

Recommendations for a Standardized Program Management Office (PMO) Time Compliance Network Order (TCNO) Patching Process

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Czumak III, Michael, Lieutenant, USAF

5d. PROJECT NUMBER
Not Funded

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/07-M8

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Network Operations Center
Detachment 1, Eighth Air Force
Attn: Capt J. Tyler McDade
245 Davis Ave
Barksdale AFB, LA 71110 DSN: 781-7235

10. SPONSOR/MONITOR'S ACRONYM(S)
AFNetOps

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Network security is a paramount concern for organizations utilizing computer technology, and the Air Force is no exception. Network software vulnerability patching is a critical determinant of network security. The Air Force deploys these patches as Time Compliance Network Orders (TCNOs), which together with associated processes and enforced timelines ensure network compliance. While the majority of the network assets affected by this process are Air Force owned and operated, a large number are maintained by external entities known as Program Management Offices (PMOs). Although these externally controlled systems provide a service to the Air Force and reside on its network, the TCNO processes for these assets are dictated and managed, to a large extent, by the PMOs. There is no current or planned, standardized method to release TCNOs to PMOs within the AF. While AFI mandates that PMOs are responsible for establishing procedures to evaluate applicability to their systems, there are no quality checks, standardization requirements or oversight to ensure the results of such evaluations are sound. Nonetheless, these PMO systems directly impact the security of the Air Force Network and the Department of Defense at large. By examining existing PMO patch management processes, this study should provide a better understanding of the TCNO processes used by PMOs with the intent of exploiting strengths and addressing weaknesses in an effort to move towards a standardized TCNO patching process.

15. SUBJECT TERMS
Time Compliance Network Order (TCNO), Program Management Office (PMO), patch management, network security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Michael R. Grimaila, PhD
U	**U**	**U**	**UU**	134	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636 x4800