NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ENHANCING DEFENSE NETWORK OPERATIONS CENTERS THROUGH THE USE OF PRIVATE SECTOR MONITORING TOOLS, APPLICATIONS, PROCESSES, AND PROCEDURES

by

Cullin R. Smith and Sean F. Docherty

June 2021

Thesis Advisor: Anthony Canan
Second Reader: Glenn R. Cook

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2021	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE ENHANCING DEFENSE NETWORK OPERATIONS CENTERS THROUGH THE USE OF PRIVATE SECTOR MONITORING TOOLS, APPLICATIONS, PROCESSES, AND PROCEDURES	5. FUNDING NUMBERS
6. AUTHOR(S) Cullin R. Smith and Sean F. Docherty	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

The effectiveness of a defense enterprise network can be directly related to that network's consistent availability and resiliency against incidents resulting in the degradation of systems and services. The 2012 Department of Defense's (DOD) Information Enterprise Architecture version 2.0 reinforced this concept by identifying that enterprise-wide access to network services and network optimization were two of the most vital aspects of an effective enterprise network. Additionally, the 2017 *National Security Strategy* (NSS) identified the requirement to improve the resiliency of federal enterprise networks. The NSS recognized that the DOD must utilize the private sector's latest applications and techniques to improve the DOD's ability to provide uninterrupted secure network services. Lichtenthaler's 2018 qualitative study in *Journal of Strategy and Management* concluded that many of the world's most innovative companies resided in the United States. The DOD may stand to benefit by collaborating with U.S. private industry to identify network incident response tools, services, and operating procedures to accomplish the effective management, monitoring, and security of defense enterprise networks. The intellectual capacity of private industry must be leveraged through public and private cooperation to enhance the DOD's ability to successfully respond to the multitude of adverse events that negatively impact defense enterprise networks.

14. SUBJECT TERMS incident handling, incident management, adverse event, outage, network vulnerability, monitoring tools, cloud computing, monitoring procedures, agile, waterfall, business process, enterprise network, cyber security	15. NUMBER OF PAGES 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ENHANCING DEFENSE NETWORK OPERATIONS CENTERS THROUGH THE USE OF PRIVATE SECTOR MONITORING TOOLS, APPLICATIONS, PROCESSES, AND PROCEDURES

Cullin R. Smith
Captain, United States Marine Corps
BS, United States Naval Academy, 2012

Sean F. Docherty
Major, United States Marine Corps
BA, Rowan University, 2008
MPS, Pennsylvania State University, 2016

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

and

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Anthony Canan
Advisor

Glenn R. Cook
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

Glenn R. Cook
Academic Associate, Graduate School of Defense Management

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The effectiveness of a defense enterprise network can be directly related to that network's consistent availability and resiliency against incidents resulting in the degradation of systems and services. The 2012 Department of Defense's (DOD) Information Enterprise Architecture version 2.0 reinforced this concept by identifying that enterprise-wide access to network services and network optimization were two of the most vital aspects of an effective enterprise network. Additionally, the 2017 *National Security Strategy* (NSS) identified the requirement to improve the resiliency of federal enterprise networks. The NSS recognized that the DOD must utilize the private sector's latest applications and techniques to improve the DOD's ability to provide uninterrupted secure network services. Lichtenthaler's 2018 qualitative study in *Journal of Strategy and Management* concluded that many of the world's most innovative companies resided in the United States. The DOD may stand to benefit by collaborating with U.S. private industry to identify network incident response tools, services, and operating procedures to accomplish the effective management, monitoring, and security of defense enterprise networks. The intellectual capacity of private industry must be leveraged through public and private cooperation to enhance the DOD's ability to successfully respond to the multitude of adverse events that negatively impact defense enterprise networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

API	application programming interface
ASI	authorized service interruptions
CSP	cloud service provider
CNAF	Commander, Naval Air Forces
CNSS	Committee on National Security Systems
COOP	continuity of operations
DDOS	distributed denial of service
DOD	Department of Defense
FAA	Federal Aviation Administration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
HIPAA	Health Insurance Portability and Accountability Act
IA	information assurance
IDPS	intrusion detection and prevention system
IT	information technology
ITIL	Information Technology Infrastructure Library
MCEN	Marine Corps Enterprise Network
NATOPS	Naval Air Training and Operating Procedures Standardization
NIST	National Institute of Standards and Technology
NSS	*National Security Strategy*
OJT	on the job training
OMB	Office of Management and Budget
PCI	Payment Card Industry
PQS	Personnel Qualification Standards
RFP	request for proposal
SAAS	software as a service
SLA	service level agreement
SP	special publication
T&R	Training and Readiness
TTP	tactics, techniques, and procedures

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank each research participant who took the time out of their frenetic schedules to provide invaluable insight into their respective organization's incident handling policies and procedures. Without the abundance of support received by organizations from private industry, academia, and the U.S. federal government, we would not have accomplished our research endeavors.

We recognize that each participant dedicated hours of support to our research through the completion of individual questionnaires and interviews. Members of the Business Executives for National Security and other private industry participants went above and beyond what was expected to provide real world examples and industry insight critical to this research. Similarly, participants from the U.S. federal government welcomed us into their facilities and provided carte blanche access to their leadership, incident handling, and computer security professionals. We feel privileged to have worked with such knowledgeable and welcoming participants during the course of this research. Based on the support we received, we remain optimistic that public and private cooperation within the United States will continue to strengthen our nation's military capabilities well into the future.

THIS PAGE INTENTIONALLY LEFT BLANK

I. RESEARCH BACKGROUND AND PURPOSE

A. INTRODUCTION

From the deep fight to rear area operations, there is little evidence to deny the importance information systems have in all aspects of military operations on the modern battlefield. Therefore, the ability to effectively manage critical information systems in garrison and abroad has become increasingly relevant within the Department of Defense (DOD) and its enterprise networks. If defense organizations are to guarantee near seamless availability of the enterprise networks that support the complete range of military operations, the implementation of new, innovative incident handling tools, services, and operating procedures must be a priority. Fortunately, the United States enjoys the benefit of being home to some of the most innovative and successful technology companies in the world. An analysis the U.S. private industry's incident handling operations is the first of many steps needed in the DOD's pursuit of enhancing network incident handling capability in support of the modern warfighter.

1. Topic Overview

The problems associated with incident handling operations are not new, nor are they simple by any means. An organization's ability to prevent and respond to an outage or service degradation involves all business sectors and facets of the organization, from human resources to executive leadership. This diverse involvement and level of complexity means that there are unfortunately no practices that can be deemed "the best" when solving these problems. Industry, use case, size, and legal responsibility are just a few of the factors that can shape the policies and procedures an organization implements for its enterprise-level network incident response. While the concept of a best practice is difficult to define given the complex socio-technical systems involved, there are practices and procedures that have deep and tangible commonality in all applications of network incident handling operations. These common threads that can be seen across industries provide a baseline from which organizations can then adjust the scope of their own needs and capabilities based on their individual use case. The goal of this research is to find those common threads

with the intention of increasing the agility and overall resilience of defense enterprise-level networks within the DOD.

The difference between an enterprise and an organization in the context of this research is not well defined and can often result in confusion. For the purposes of clarity, an enterprise will reference a grouping based on a systems or network-level mindset as in the Marine Corps' Enterprise Network (MCEN). Conversely, an organization is a logical concept of organization that can be larger than a given enterprise (such as the entire DOD), or subdivisions within a larger organization all serviced by a common enterprise (such as individual units all operating on the MCEN). Throughout this research, the relative scale of organizations referenced, and their associated enterprise environments, is not consistent, but is instead unique to the individual entity. For the most part, the recommendations and points of view expressed in this research are from the perspective of branch-level enterprise networks within the DOD, with the understanding that these enterprises serve many smaller organizations, each with their own missions, organization, and systems. The scale and relationship between the organizations and their enterprise networks and systems are important concepts to consider as the practices extoled for a given organization or enterprise may not be tenable for another.

While the thought of closely examining organizational business practices with the intent of improvement may seem like an evaluative measure, this research is not an audit. The incident handling methods observed in this research, the metrics by which incident response is measured, and the efficacy of those methods and metrics are all self-identified by the individual participants. To attempt to hold each organization and its capabilities against a universal model of best practice is neither possible nor practical. Instead, this research should be used as a means to highlight the core of what constitutes state-of-the-art technologies and practices at the time of writing. Changes in technology, advancements in business practices, and shifting philosophical paradigms that dictate how network incident handling operations are executed will continue to reshape the landscape of network incident response and security, potentially making a subset of the conclusions found within this research obsolete in the future. The researchers seek to achieve an understanding of what is being done at the time of research by those at the forefront of the

field. It is therefore vitally important that business executives, IT managers, policy makers, and leaders at every level continue to adhere to a maneuver warfare mindset by encouraging continued research and remaining knowledgeable in this changing domain.

2. Participation Overview

To ensure that the research included a diverse range of participants, the research sampling included organizations that varied in industry, size, and structure. On one end of the spectrum, participants included robust cloud service providers (CSP) and software as a service (SaaS) companies like Microsoft as well as members of the automotive and airline transportation industries. These larger organizations were, in many ways, representative of Defense Enterprise Networks in that each organization provided enterprise network services to thousands of customers. On the other end of the spectrum, participants included multiple tech startups and public universities. These organizations were included in the sample, recognizing that they too may be implementing security and incident handling tools, practices, and procedures relevant within DOD enterprise networks. The sample also included an array of U.S. federal government organizations and DOD enterprise networks, including input from two of the four largest enterprise networks in the DOD. As seen in Tables 1 and 2, the total number of participants was thirteen, including eight organizations from the private industry and academia and five from the federal government.

Table 1. Participant Industry Breakdown

Industry Represented	Number of participants
Government	5
Service Providers / SaaS	3
Academia	2
Transportation	2
Security and Consulting	1

Table 2. Participant Size Breakdown

Organization Size	Number of Participants
Small (Up to 1,000 users)	2
Medium (1,001 to 25,000 users)	4
Large (More than 25,000 users)	7

3. Research Methodology

The research used a qualitative methods approach to examine both the federal government and private industry's incident handling operations policies, procedures, and tools. The first phase of the analysis was a qualitative review of existing literature. The research focused on literature released over the last two decades by both the federal government and private industry. The two-decades timeframe was chosen for two reasons: (a) starting in the early 21st century, computer and information scientists began to review network-monitoring practices with intellectual rigor intent on establishing long-term solutions; and (b) the proliferation of technically advanced and geographically distributed networks over the last decade makes literature produced before this particular time period less relevant for the current operating environment. As a result, the literature review will use the year 2000 as a baseline for further research.

The goal of Phase I analysis was to establish the baseline characteristics and concepts included in federal government security and incident handling policies, as well as the similarities and differences that exist between these U.S. federal policies and what was being implemented by private industry. After all concepts were consolidated, researchers conducted a comparative analysis to identify thematic trends that existed across the U.S. federal government and private industry models. Following the completion of the analysis, a 61-question questionnaire (see the appendix) was created that segmented operational domains within the incident-prevention and incident handling industry into four distinct categories: Policies, Methodologies, Structure, and Standards; Personnel, Training, and Network Operations Center Structure; Incident Identification Tools and Procedures; and Program Management Techniques. The questionnaire was created using the network incident handling operations industry standards identified by the National Institute of Standards and Technology (NIST) 800 series of special publications, emphasizing NIST's

security (SP 800–53) and incident handling (SP 800–61) frameworks (Cichonski et al., 2012).

Phase II of the research included the examination of individual use-cases. This examination occurred in three different forms: on-site security and network operations center visits, virtual synchronous interviews, and asynchronous questionnaire completion. Whether conducted in-person or virtually, each method of evaluation leveraged the research questionnaire and analyzed the security and network incident handling tools, policies, processes, and procedures being used by each participant. Site visits were extremely thorough and included interviews with each individual section of an organization's network operations model. These sections included network operations, incident handling, helpdesk activity, defensive cyber teams, security operations, and organizational leadership. During synchronous virtual interviews, the researchers coordinated with organizations to ensure that members from each relevant section of their respective incident handling operations were available for the interview. During asynchronous questionnaire completion, participants typically leveraged organizational wikis and other collaboration tools to ensure that the appropriate personnel were providing the input necessary to complete the questionnaire in a detailed and accurate manner.

Phase III included a thematic analysis of all completed questionnaires. The data was analyzed for thematic outliers and inconsistencies that existed between U.S. private industry and federal government's incident response operations. Researchers then created a model that separated data into the phases of the incident handling life cycle. NIST Special Publication 800–61 identified that incident handling teams execute operations in one of four stages: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity (see Figure 1). The researchers also added "Policy" as a fifth stage in the incident handling life cycle, recognizing incident handling policy as a pre-requisite necessary to successfully execute all other stages. The fifth stage of the life cycle was added primarily due to the legal and organizational implications different policies had on incident handling methodology and decisions that were realized during the data analysis phase. By segmenting the data into the five phases of the incident handling life cycle, the researchers identified the frequency with which public and private organizations' incident

handling methodology aligned with NIST recommendations within each individual stage. However, instead of creating a performance metric that simply measured this frequency, the researchers investigated the instances in which participants deviated from NIST recommendations, attempting to potentially identify a state-of-the-art practice or procedure not yet identified within U.S. federal policy.

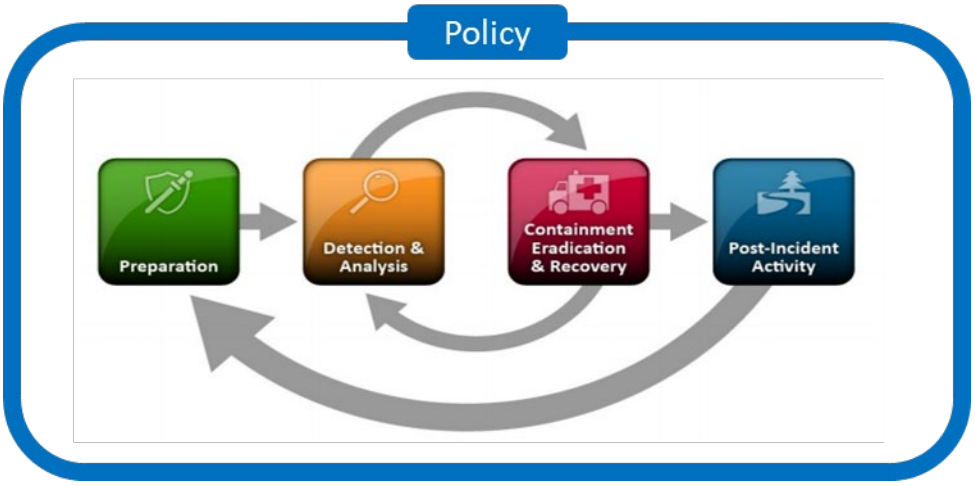

Figure 1. NIST Incident Handling Life Cycle and Policy Relationship. Adapted from Cichonski et al. (2012).

4. Research Goals and Intent

The analysis conducted in this research used NIST's incident handling guide as a framework with the addition of an in-depth analysis of network and incident handling policy. The addition of this policy analysis was derived from the recognition of the importance organizational policy plays on all aspects of incident handling as outlined in NIST's guide. The research will conclude with a list of recommendations pertaining to incident handling policy, procedures, and tools that may potentially enhance the agility and resilience of DOD enterprise networks, to include the MCEN. Recommendations will be formulated based on the frequency with which a particular practice or methodology was mentioned in the research sample, instances of procedural success that were self-identified by participants, capability short-falls expressed by participating organizations, and the current state of the art based on studies and techniques developed during past research

efforts. The most recent *National Security Strategy* (NSS) (2017) advocates for public and private cooperation to enhance the security of the nation's critical infrastructure, including the government's enterprise networks. This systematic review and thematic analysis of incident handling practices in both the federal government and U.S. private industries will focus on identifying the unique requirements and use-cases within the DOD to determine the applicability of the private industry's most efficient incident response practices. The goal is to determine the applicability of these changes within the DOD's enterprise operations communities.

B. U.S. FEDERAL GOVERNMENT POLICY AND INCIDENT HANDLING FRAMEWORK

In 2000, the White House recognized the strategic importance of the United States' network infrastructure as it applied to federal government agencies' ability to carry out the NSS. This realization led to the release of The Office of Management and Budget's (OMB) Circular no. A-130, Appendix III, which had two primary objectives: The first objective was to identify federal government information systems as a strategic resource; and the second, was to establish the capability to support network users when a security incident occurs (Office of Management and Budget [OMB], 2016). In 2002, two years after the release of the White House's circular, Congress signed the Federal Information Security Modernization Act (FISMA) into law, officially mandating that federal government organizations implement policies and procedures for incident detection, reporting, and response (E-Government Act, 2002). Together, these two documents established the legal precedent for the implementation of federal government incident prevention and handling policies.

1. The Origins of NIST's Incident Handling Guide

Within FISMA, NIST was explicitly tasked to establish security definitions, controls, and an incident handling framework that U.S. federal agencies would leverage when developing their cyber security (incident prevention) and incident handling policies. It is from here that the current iteration of the Federal Information Processing Standards (FIPS) and NIST 800-series Special Publications (SP-800) originate. The 800-series

Special Publications developed by NIST and their parent laws and directives make up an overarching policy and framework that systems critical to national security must follow. While organizations within the federal government have additional overlays, orders, and standard operating procedures that help to tailor incident handling policy to the needs of that individual organization, these additional policies must exist within the bounds of NIST's framework, adding specificity and additional requirements specific to the systems and missions they address.

The security and incident handling frameworks developed on behalf of the U.S. federal government by NIST, derive both their origin and authority from public policy and U.S. federal law. As such, the controls and standards outlined in these frameworks impose legal requirements on all systems deemed critical to national security. While other security and incident handling frameworks are being used successfully by organizations around the world, NIST's incident handling framework is used throughout this research as a baseline because of the legal implications NIST's framework has on National Security Systems. This chapter will briefly examine the origins and broad concepts outlined in NIST's security and incident handling frameworks as they apply to DOD's Enterprise Networks and the MCEN. The intent of this section is to present the lens through which this research was conducted, and the resulting recommendations are made. This lens specifically targets DOD organizations operating national security systems and their associated defense enterprise networks. However, the underlying concepts outlined below are in no way unique to NIST's framework, and the recommendations presented in later sections can still be applied to organizations and enterprises that do not adhere to NIST publications directly.

2. The NIST Incident Handling Life Cycle

The NIST incident handling guide establishes that incident handling occurs in four distinct stages, as shown in Figure 1: 1) preparation, 2) detection and analysis, 3) containment, eradication, recovery, and 4) post-incident activity (Cichonski et al., 2012). In addition to the incident handling stages as defined by NIST, this research establishes policy as a stage zero because of the researcher's assessment that organizations must implement incident handling policy to effectively execute all other stages within NIST's

model, and the prevalence of policy adoption and implementation that was found during data collection. Following the development and implementation of policy, the preparation stage serves as an organization's opportunity to identify the incident handling team structure most suitable for their use-case and train their incident handlers (Cichonski et al.). The preparation phase also focuses on preventing incidents by implementing controls that enhance enterprise systems, network, and applications security as referenced in NIST's Security and Privacy Controls for Information Systems and Organizations, SP 800–53 (Cichonski et al.). NIST recommends that government incident handling teams establish an array of facilities and on-hand information to include network diagrams, issue tracking systems, and other key capabilities during the preparation stage (Cichonski et al.). These additional tools are critically important for incident handlers during their response to future incidents.

Following the conclusion of the preparation stage, NIST recommends that incident handling teams focus on mitigating the impact of future incidents during the detection and analysis stage. NIST suggests that incident handling teams leverage the security standards and protocols referenced in NIST Special Publication 800–53, Federal Information Processing Standards (FIPS) Publications, and the Committee on National Security Systems (CNSS) Instruction 1253, to enact robust preventative measures. However, incident handling teams must have the monitoring and notification tools and procedures necessary to identify and respond to the adverse events that inevitably do occur. NIST's incident handling guide identifies that for many organizations the most difficult task involved with the incident handling process is accurately detecting and assessing potential incidents (Cichonski et al.). During the detection and analysis stage, incident handling teams leverage their suite of tools and organic experience to identify and respond to an incident's early warning signs. When implemented effectively, monitoring and detection tools, notification escalation hierarchies, and incident prioritization and categorization methods can assist an incident handling team with quarantining, eradication and service restoration efforts.

Once an incident has been confirmed and the appropriate analysis is complete, incident troubleshooting, containment, and eradication are often tied to and directed by an

organization's incident categorization policy. Incident prioritization and categorization are the results of careful analysis of the risks and impact levels associated with a given system or set of systems (Cichonski et al.). Whether an organization is experiencing a basic Internet Protocol outage, malware infection, or Distributed Denial of Service (DDoS) attack, the incident handling and containment procedures will be characterized by actions and timelines identified in the prioritization policy (Cichonski et al.). As outlined in NIST's Risk Management Framework for Information Systems and Organizations, the prioritization and containment guidelines instituted by an organization typically result from an analysis of the likelihood of damage to the network, exploited resource classification levels, critical core service requirements, and restoration timelines (NIST, 2018). A clear understanding of incident prioritization and system impact categorization is vital for an effective incident handling team to be able to ensure operational continuity despite a system degradation. In most organizations the containment and eradication processes occur in a tiered response structure. Coimbatore Chandersekaran and William Simpson, authors of "A Multi-tiered Approach to Enterprise Support Services" (2011) identified these tiered levels of troubleshooting support as levels 0–3. Level 0 represented user self-help technologies, Level 1 represented basic help desk support to include over-the-phone and chatroom troubleshooting techniques, Level 2 represented proactive monitoring techniques and engineering services that required advanced troubleshooting capabilities, and Level 3 represented active monitoring and security capabilities; Level 3 technician's may conduct on site physical troubleshooting and could potentially include contracted vendor support (Chandersekaran & Simpson, 2011). This tiered incident response strategy presents a succinct method for incident handling teams to organize their containment and eradication capabilities.

NIST identifies that incident recovery does not stop after normal system operation has been restored. During the post-incident activity stage of the incident handling life cycle, the remediation and documentation of vulnerabilities is an ongoing task that falls within the responsibilities of incident handling personnel to prevent similar incidents in the future (Cichonski et al.). Following an incident NIST recommends that organizations focus on learning and improving through the use of a "lessons learned" meeting with all parties that

were involved in the handling of the incident (Cichonski et al.). Post-incident activity should detail any characteristic of an incident or it's handling that either inhibited timely recovery or successfully mitigated the impact of the event. NIST identifies that the collection and analysis of lessons learned information is only one step to effectively completing the post-incident activity stage, organizations must also use that collected data to implement new policies and procedures to continue to enhance their response to future incidents (Cichonski et al.).

3. NIST's Relationship to Other Frameworks

These incident handling principles outlined by NIST are pertinent to the requirements imposed by public policy on the MCEN as they establish the baseline for recommendations for improvement to the incident handling process within a given DOD Enterprise Network. It is important to note that there are a significant number of other security and incident handling frameworks used by the private industry that have been developed by trade organizations, financial regulatory bodies, and for-profit audit and certification organizations. These other frameworks were created to meet needs within specific sectors of industry. While each of these frameworks have their own nuances and implementation paradigms, they draw from the same fundamental security and incident handling concepts upon which NIST has drawn in the development of their framework. As findings are presented throughout this research, the differences found in these other frameworks as they apply to participating organizations will be identified. Analyzing and understanding the frameworks and implementations observed in private industry may have a great deal of relevancy to the MCEN, despite the strict requirements imposed on federal government organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FINDINGS

A. NIST AND ORGANIZATIONAL INCIDENT HANDLING POLICY

In this section, results and findings from interviews and questionnaires are organized and presented according to how they pertain to the different stages of NIST's incident handling life cycle. The one exception to this being the inclusion of an initial stage zero on policy, which was added due to the role which policy plays directly or indirectly in how an organization responds to an incident. NIST's incident handling framework omits any direct discussion on policy because the NIST principles and framework were originally developed for the express purpose of implementation on U.S. federal information systems, making usage of U.S. federal policy a given. This chapter on policy primarily addresses some of the differences in stated policy from that which is observed, as well as explores other policies and frameworks not developed by NIST observed during research. Following the chapter on policy, findings are organized by first addressing the preparation and protection phase of the incident handling life cycle and then followed by detection and analysis, containment, eradication, and recovery, and finally post-incident activity. In this section when specific organizations are referenced, they identified only by their industry or business sector due to the number of participants that expressed a desire to remain anonymous.

1. DOD Policy Adoption

Despite requirements imposed on the DOD by the succession of congressional directives mentioned previously it is surprising to find how infrequently participating DOD organizations were aware of the frameworks developed by NIST or policies outlined in the Federal Information Security Act. In the course of this research, only 40% of participating federal government organizations mentioned any adherence to U.S. federal government policy, outside of directives and standard operating procedures that were developed at the local level. Within the other 60% of participating organizations, this research found that network operators and incident handlers followed local directives and procedures with little knowledge or understanding of parent directives developed at higher echelons of

command. While local procedures and directives can and should be developed in order to fill gaps and provide specificity unavailable in parent policies, those policies from which local procedures are derived should still be referenced and maintained in order to establish a foundation of consistency and clarity. In the cases where the federally mandated framework was not commonly used, participating organizations referenced frameworks and procedures outlined by the Information Technology Infrastructure Library (ITIL) or other third parties than those mandated by Congressional policy (Agutter, 2019).

In many cases, the frameworks developed by ITIL and other third parties that are being used by DOD organizations meet or exceed the minimum requirements defined by NIST. Additionally, implementing a hybrid framework which knits together concepts from multiple sources is certainly a viable solution as will be explored in the following section. However, the most concerning finding among participating DOD organizations that are using these non-NIST frameworks, is that the derived policies being used at the local organization level are so far removed from federally-mandated policies and practices, that network operators and incident handlers are now unaware of their origin. These findings point to two major systemic issues. The first is an overall lack of standardization and accountability among DOD organizations with regards to networks and IT systems. While NIST is charged with providing a standard for U.S. federal government organizations to follow, adherence to that standard is left to leadership within each branch and is not tightly controlled or enforced by a central entity. Without external accountability, these organizations have little incentive to conform to federally mandated policy. Second, services within the DOD have historically operated disparate networks with little need to integrate with one another, thus eliminating the requirement for a standardized approach when it comes to network incident handling. The vestiges of this siloed approach have inevitably led to a culture of self-conformity, resulting in inconsistency and hindered interoperability.

2. Customer-Driven Hybrid Policies

Ironically, participants within private industry and academia were far more eager to comply with the NIST incident handling framework (62.5%); though, compliance

occurred as a result of very different motivating factors than their counterparts within the federal government. The decision to adhere to a given policy and meet certain compliance metrics within the private industry and academia was almost entirely driven by their given customer-base. In the case of those participants that did business with the federal government, this meant adherence to NIST and FISMA regulation was required. In the case where participants did business with the banking industry, healthcare, or domestic aviation, this resulted in similar compliance with Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Federal Aviation Administration (FAA) practices and standards. Additionally, several for-profit organizations have developed other frameworks and standards that are being used by the private industry in a best-practices capacity which meet or exceed those standards required by NIST. While such an eclectic hybrid approach is neither required nor viable for federal government organizations, the fact that 87.5% of participants within private industry and academia have managed to use hybrid frameworks, many of which incorporate NIST standards (62.5%), shows the viability of this approach in real-world applications. The question then becomes whether this hybrid paradigm is what some DOD organizations were attempting all along, but somehow fell short in implementation along the way? In either case, the choice to adopt a hybrid approach should be made with a complete knowledge and understanding of what is outlined in U.S. federal law, providing a foundation upon which other policy decision can be made. There is little evidence that NIST was used as a foundation when other frameworks were adopted by DOD organizations, which makes earlier conclusions about the lack of NIST compliance much more likely.

3. The Role of Service Level Agreements

Despite differences in approaches to policy and incident handling framework implementation, one these that was found to be critical among all participants was the impact and role played by service level agreements (SLAs). All participants in both government and private organizations mentioned that some subset of capabilities was being outsourced to some degree, and that outsourcing involved an SLA in some capacity. Additionally, all participants noted the inherent tradeoffs between capability, cost, and speed when dealing with external service providers or contractors during the incident

handling process. When participants responded about interactions with these service providers, they all alluded to the fact that having contact with engineers or experts for a particular service or system was a worthwhile capability. The contributions provided to an organization's ability to troubleshoot and integrate a particular system with the larger whole was the primary motivation for engaging as-a-service type contracts and, when funding was available, have some sort of expert on retainer. However, the main deterrent from simply outsourcing everything was speed and cost. Every time an incident handler was required to go outside of the organization to engage a contractor or help desk for an external resource or system, the incident handling process was noted to be appreciably slower. This can be a significant issue for time and mission critical systems, a risk that was mitigated by some participants through geographically collocated contracted support personnel, or access to near real-time communications with service providers. There are two major inhibitors noted by participants when it comes to contracted services and SLAs: First is that this support comes at a monetary cost that can easily be prohibitive. Second, having an unclear understanding of responsibilities between service providers and incident handling personnel can also lead to a swift unraveling of intended benefits, leaving incident response teams between Scylla and Charybdis.

From a cost perspective, participants mentioned support for services ranging from a limited number of remote helpdesk hours available to having employees from supporting organizations on site in a fulltime status and everything in between. The general consensus (66.6%) among participants was that one often gets what one pays for in that regard. While the latter service model is robust and immediate, it was often prohibitively expensive for all but the largest organizations with the most to lose for a given outage. In one case in particular, a major cloud service provider has begun to limit the number of full-time contractors for certain systems; instead, opting to pay for system-specific training or simply hire system experts outright as a cost-saving measure. At the other end of the spectrum, 50% of participants that had very basic levels of service also identified a noticeable increase in the overall timeline for a given outage that involved external support or services. The decision to opt for a more robust support package was often tied to system and service prioritization and an organization's own responsibilities to their customers. This means for

many participating organizations multiple service level agreement models and support packages were in effect, and each was based on restoration and support requirements of individual systems. Depending on the size of the organization and the complexity of systems they operate, this network of SLAs can quickly become complicated and unwieldy.

In general, participants within the private industry were more effective in managing SLAs and the responsibilities of service support personnel at the network operations and incident handling personnel level. This is primarily because these participants tend to be flatter in their organization, with fewer levels of obscuration between those who develop and implement SLAs, and those who interact with the systems those SLAs involve. There is certainly precedent for robust and well-managed SLAs within federal government organizations. However, there tended to be less control over the SLAs at an operational level and 40% of participants within the federal government expressed past issues where SLAs were not specific or adequate enough to eliminate ambiguity in responsibility. In order to maximize the effectiveness of contracted or service provider support, 83.3% participants identified the need for clearly defined and understood SLAs that appropriately delineate areas of responsibility and performance metrics for both the supporting and supported parties both internal to the organization and externally. Having robust policies and SLAs in place from the outset provides a stable platform upon which operational decisions and incident handling practices are built. Once the incident handling life cycle is in motion, little can be done to attempt to fix inadequate policy decisions post-hoc.

B. NIST AND ORGANIZATIONAL INCIDENT HANDLING PREPARATION

As part of the adoption and implementation of the appropriate policy, organizations must begin to execute preparatory actions to ensure they are ready to respond to adverse events impacting their users. As such, the implementation of sound incident preparation and prevention procedures is critical to the success of an incident handling team. NIST recognizes that even when recommended security controls are in place, incidents cannot be eliminated completely. This chapter will provide a comprehensive review of the preparatory steps necessary to build a proactive incident response capability as identified

in NIST's incident handling guide, as well as the unique perspectives from several participants within the research sample.

1. Incident Response Plans, Policies, and Procedures

Although incident response plans, policies, and procedures are typically nuanced based on individual use-cases; NIST offers overarching incident response concepts that may be applicable across multiple industries. The NIST incident handling guide recommends that organizations define the roles, responsibilities, and authorities of their incident response team prior to implementation (Cichonski et al.). The goal is to identify the scope of services to be provided by the incident handling team and transparent operating lanes in which incident handlers can successfully perform their duties. Despite differences in the business objectives that drive incident handling policy among U.S. federal government organizations, NIST recommends that at a minimum the following elements be included in each organization's policy:

1. A statement of management commitment.
2. The purpose and objectives of the policy.
3. Definition of computer security incidents and related terms.
4. Organizational structure and definition of roles, responsibilities, and levels of authority.
5. Prioritization or severity ratings of incidents.
6. Performance measures.
7. Reporting and contact forms (Cichonski et al., p. 8).

Especially important in NIST's recommendations is the implementation of incident severity scores or ratings. It is common for incident handling teams to become overwhelmed with the sheer volume of notifications, missing critical threats and outages in the process. Incident handlers must be prepared with transparent incident severity scorecards to establish an incident rating immediately to categorize the incident and initiate the troubleshooting process.

Several of the participants from the research sample (77%) implemented incident handling policies and procedures that are nearly identical to that recommended by NIST's incident handling guide. Every organization in the sample created well-defined policies and procedures that guide incident handling requirements for their incident handling teams. All research participants within private industry leverage NIST's recommended concepts in some fashion; however, only 40% of the U.S. federal government organizations interviewed were familiar with the concepts recommended in NIST's incident handling guide. This result was surprising; several of the individual spokespersons from U.S. federal government organizations even admitted to being unaware of NIST's incident handling guide. As discussed earlier, the major differentiator between public and private organizations' incident handling policies was that private organization policy was largely guided by contractual agreements or SLAs while U.S. federal government organizational policy is guided by hierarchical regulations.

Critical to organizational incident handling policy is incident rating and categorization procedures. Every participant had established an incident rating and categorization policy; however, the details requisite to each policy varied significantly. Each participant within private industry reported that SLAs played a critical role in determining incident prioritization and categorization for services provided to their customers. One participant, a cloud service provider, offered that categorization and scoring are typically focused on the value of the asset (system or service) being threatened or degraded. That same participant offered that the actor performing the exploitation also factors into an incident's priority level. On the other hand, U.S. federal government participants tended to rely on metrics-based rating and categorization policies. These organizations focused on variables including number of users impacted, geographic area impacted, and the type of service being impacted. All U.S. federal government organizations had developed policies that identified an enterprise service as non-mission critical or critical core. Multiple U.S. federal government organizations suggested that incident troubleshooting is typically carried out by contracted vendor support, and incident rating and categorization policy agreed upon within SLAs inevitably determines how a vendor will respond to an incident. One such participant suggested that contractual

agreements written two to three years in the past may not account for new technologies that their users have become reliant on, hence incident rating and categorization should always remain negotiable.

The introduction of new technologies has resulted in a strategic transition to cloud-based incident handling models. All participants reported that at least one of their incident handling services was now primarily available via a cloud-based solution or, at a minimum, contracted to an agency that was operating the service in the cloud. As a result of this transition, incident handling teams have become increasingly dependent on off-premise personnel and network infrastructure to carry out their incident handling procedures. Participants from both U.S. federal government organizations and the private industry alluded to the fact that cloud-based incident handling architectures allowed for interoperability, scalability, ease-of-use, information sharing, and enhanced collaboration. However, the transition has not occurred without drawbacks. Amongst other negative outcomes, U.S. federal government participants admitted to the fact that reliance on off-premise technicians has at times resulted in troubleshooting delays. One government organization explained that relying on vendors to solely troubleshoot service outages has resulted in delays as significant as six months.

2. Incident Handling Team Structures

One facet of an incident handling model prioritized by NIST is the creation of an incident handling team, or the personnel responsible for carrying out incident handling procedures. NIST identified that in most instances, incident handling teams require a manager, technical lead, and incident handlers (Cichonski et al., 2012). NIST recommends that team members have a wide range of technical and interpersonal skills including network administration, programming, technical support, and intrusion detection, as well as teamwork and communications skills (Cichonski et al.).

NIST's incident handling guide offers that incident handling teams are not intended to be self-sufficient; teams require support from several other groups within their respective organization. Executive management support is amongst the most important. Executive management is typically responsible for staffing, budgeting, and establishing policy, which

are all critical elements when implementing an incident handling capability (Cichonski et al.). This characteristic of incident handling makes executive management support critical to the success of an incident handling team (Cichonski et al.). Incident handling teams also require assistance from Information Assurance (IA) and Information Technology (IT) specialists (Cichonski et al.). Security incidents nearly always require IA specialists who can perform containment, eradication, and recovery techniques. While other network-related incidents require advanced troubleshooting and network configuration, these troubleshooting steps are typically performed by IT specialists. Incident handling teams should also consider adding subject matter experts with legal, public affairs, human resources, physical security, and business continuity experience (Cichonski et al.).

NIST's incident handling guide also suggests various incident handling team models based on the size and mission of the organization. NIST recommends that small organizations leverage a centralized incident response team structure. In this type of structure, one incident handling team is geographically collocated and is responsible for resolving incidents throughout an organization (Cichonski et al.). For larger organizations, NIST recommends using a distributed incident response team, wherein multiple support teams are distributed geographically within an organization to support regionalized users (Cichonski et al.). Finally, NIST has found that some organizations may benefit from the development of coordinating teams or a team of teams, wherein a centralized incident response team provides advice to smaller disaggregate teams within an organization without having direct authority over those teams (Cichonski et al., 2012).

Participant incident handling team sizes varied significantly as a result of the research sample's diverse participant pool. Teams ranged in size from more than one-hundred members for one participant, to three members for another. One common theme that nearly every participant indicated was that incident handling teams are becoming increasingly disaggregate; 77% of participants indicated that their teams were located in several regions across the globe or even working from home. One of the larger participants, a software-as-a-service company, noted that implementing a disaggregate model allows organizations the opportunity to hire incident handlers and technicians who are located around the world. The organization suggested that the days of relying on an applicant pool

within the general vicinity of your company's headquarters are gone. Organizations can now look for unique talent and skills across the globe to create an increasingly effective remote workforce.

Incident handling teams within the sample also had an eclectic range of professionals serving within each respective team. As NIST recommended, incident handling teams from nearly every organization included at least one IA, IT, and security professional; however, there were a few unique capabilities that organizations decided to include within their incident handling teams. A few of the unique professions that were added to private industry incident handling teams were emergency management professionals, application-specific subject matter experts, and in one case, an anthropologist. One participant, a large CSP, explained that anthropologists provide incident handling teams with a different perspective on human behavior and how an attacker may be analyzing an enterprise network for vulnerabilities. One private, multi-billion-dollar organization stated that they look for former electricians and plumbers to serve as incident handlers because these applicants typically excel at troubleshooting physical device issues. While the private industry is hiring the IA and IT professionals recommended by NIST, they're also looking for unique capabilities and are thinking outside the box when assembling their incident handling teams.

One reoccurring theme from the research sample was that U.S. federal government participants were becoming increasingly reliant on contracted vendor support to assist with incident handling responsibilities. The alarming thing about this transition is that all U.S. federal government organizations also stated that incident time-to-restoration can be increased during incidents that require off-premises vendor support. Naturally, government organizations that paid vendors to physically locate incident handlers on-site, within their enterprise operations centers, indicated that these liaisons were extremely helpful. One government organization paid to have eight contracted, vendor technicians on site to support incident handling and enterprise planning operations.

3. Incident Handler Training

NIST's incident handling guide does not specifically state the type of training that incident handling teams should receive initially or annually. NIST instead includes broad training information in Special Publication 800–84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. In SP 800–84, NIST identifies that all training plans have four unique phases: Design, Development, Conduct, and Evaluation (Grance et al., 2006). NIST defines training as a continuum of learning activities that enables staff to maintain their skills and technical proficiencies (Grance et al., 2006). NIST breaks practical application training into three categories: exercises, tests, and actual emergency situations; and individual training into two categories: instructor-led and self-study (Grance et al., 2006). By implementing a detailed and well-scheduled training plan that includes both practical application events and individual training, NIST suggests that a training plan should be capable of assisting employees with maintaining and advancing their capabilities.

Although not directly mentioned in NIST SP 800-61 or NIST SP 800-84, the U.S. federal government has established compliance requirements for defense enterprise network professionals, to include incident handlers. The compliance manual that contains this information is DOD 8570.01-M, Information Assurance Workforce Improvement Program. The DOD 8570 provides guidance and procedures for the training, certification, and management of the DOD workforce conduct of IA functions (Grimes, 2005). The manual details the responsibilities carried out by IA professionals and the formal certifications necessary for personnel (civilian, military, and contractor) to receive permissions on defense enterprise networks.

The rigidity of the compliance manual does not align well with NIST SP 800-84 training recommendations. NIST recommends the implementation of a fluid training schedule that includes both practical application as well as individual study, while the compliance manual focuses on formal certification requirements. The compliance manual is likely best suited as an initial training initiative to be built upon through the implementation of practical tests and exercises. However, many of the government

participants in the research sample indicated that this is not how requirements outlined in the DOD 8570 were being treated.

The DOD 8570 details an extremely specific training pipeline for U.S. federal government employees to pursue. All U.S. federal government participants (100%) identified the DOD 8570 as their source training document. This was not the case for private industry participants. Private industry unanimously stressed the importance of experience over formal certifications and discussed how experience may be a more suitable litmus test for potential incident handling applicants' abilities. The private industry has the luxury of being able to hire anyone. Having the latitude to define hiring requirements means specific certifications are quickly being dismissed in favor of individual experience.

Although DOD 8570 compliance is required by law within U.S. federal government organizations, there are a wide range of individual certifications that could potentially meet compliance standards, and once a particular certification is achieved, there is very little in the way of continuing education, system specific certification, or defined training pipelines for advancement. As NIST SP 800-84 describes, incident handling team leadership should be evaluating opportunities to include exercise and response tests within annual training schedules. Several of the research participants (54%) admitted to focusing on individual training, whether it be instructor-led or self-study, rather than practical application. A common theme was that practical application training was often very difficult to implement on a real-world or operational enterprise network. This meant that practical application training often did not exist and was simply substituted with on-the-job training. In this training environment, incident response personnel learned using over-the-shoulder or learning through mistake training techniques.

C. ORGANIZATIONAL INCIDENT DETECTION, VALIDATION, ANALYSIS, AND NOTIFICATION

Once an incident handling team has been established and the organization's incident handlers have been trained appropriately, incident handling teams must execute the plans, policies, and procedures that have been put in place to respond to an incident. This can be a daunting process as incident handlers are often required to analyze thousands

of alerts, anomalies, and individual incidents daily. An organization's proficiency in the art of detection, validation, and early analysis can limit the severity of a service degradation's impact on operations, or possibly prevent the outage entirely.

1. Incident Detection and Validation

NIST classifies early warning signs as events that are about to occur and categorizes them into two categories: precursors and indicators (Cichonski et al., 2012). A precursor is a sign that an incident is likely to occur in the future, such as a press release identifying a new known network vulnerability (Cichonski et al.). Conversely, an indicator is a sign that an incident has already taken place (Cichonski et al.). Indicators can include computer security software alerts, anomalous log-file activity, unusual network traffic flows, or even user support requests (Cichonski et al.). To successfully identify precursors and indicators, NIST recommends the use of automated detection capabilities such as network-based and host-based intrusion detection and prevention systems (IDPS), log analyzers, and computer security software to assist incident handling teams with incident detection (Cichonski et al.). While these applications and computer security tools have become increasingly automated over the past decade, incident handlers are still expected to have requisite technical knowledge and experience to appropriately sort through the sensor and application data necessary to diagnose ongoing incidents (Cichonski et al.).

Once an early warning sign has been detected, incident handling teams must act immediately. Following early warning sign detection, the first step an incident handling team must accomplish is incident validation (Cichonski et al.). Incident validation has become increasingly difficult for incident handlers as a result of overwhelming amounts of data that must be analyzed to confirm incidents. Incident handlers typically use multiple applications to detect incidents, as a result, application notification volume has become unreasonably high. NIST identified that the notification volume for many organizations now surpasses thousands or even millions of sensor alerts each day (Cichonski et al.).

The research sample established several unique methods and various sets of tools and applications for incident detection, validation, analysis, and notification. Every research participant had established incident detection tools to identify early warning signs;

however, the tools mentioned by participants were nearly always different. Many of the sample's private industry participants had developed proprietary tool sets that were engineered specifically for their respective networks. One of the most significant findings was that 100% of private industry participants had developed or implemented application programming interface (API) technologies that proactively monitored their organization's critical applications. These tools assisted private organizations and automated the monitoring of applications most critical to users and customers.

Application monitoring represented a capability that the research sample's federal government participants were not implementing. None of the federal government participants had identified a method or technology capable of automating application monitoring services for their entire suite of critical applications. One federal government participant identified that passive application monitoring was at the top of their priority list and that they were currently in the process of requesting Request for Proposals (RFPs) from multiple vendors to provide this capability. Another federal government participant pointed out that their incident handling team was highly reliant on customer support requests to identify early warning signs of an impending incident. The participant alluded to nearly 80% of their incidents being identified by customers after the incident had already taken place. This was a common theme for federal government participants within the research sample: federal government participant incident response was largely reactive while private industry maintained a pro-active posture, identifying incidents prior to occurrence.

2. Incident Analysis

Following incident validation, teams conduct preliminary incident analysis to initiate the organization's incident notification and communication process. In these instances, it is incumbent upon the incident response team to notify the appropriate technical support agents, organizational leadership, and in some instances external agencies to include law enforcement and the media. This is precisely why the team's early analysis is so critical; incident handling teams that misdiagnose an incident may notify technical support agents incapable of troubleshooting the outage, which inevitably extends

time-to-restoration. NIST recommends that early analysis should attempt to determine the incident's scope, the networks and systems impacted, who or what originated the incident, and how the incident is occurring or the reason for outage (Cichonski et al., 2012). NIST also emphasizes the importance of communication between incident handlers and the business units they support.

After an incident had been validated, 100% of research participants established a hierarchical incident analysis and reporting posture similar to that explained in Coimbatore Chandersekaran and William Simpson's work on tiered incident troubleshooting methodology. Although participants referred to their analysis and reporting chains using various terminology, many of the participants established a tiered troubleshooting concept to respond to ongoing incidents. Nearly half (46%) of the sample's participants had implemented tiered incident response and analysis measures in some capacity. Several (60%) private industry participants had experienced a level of success automating their TIER 0 support mechanisms or user self-service support structures. This included online do-it-yourself troubleshooting portals and password recovery mechanisms in some instances. In all cases, after an incident had been identified and validated, the incident documentation process would commence and notification of the appropriate personnel, whether it be technicians, leadership, or outside agencies, would be initiated.

3. Incident Notification

NIST recommends prioritizing the incident documentation and notification process during each event using an issue tracking system. Proprietary incident tracking systems mentioned during the research questionnaire included: Remedy, PagerDuty, and ServiceNow. These systems allow incident handlers to track the progress of an incident; they typically result in fewer systematic errors by increasing situational awareness (Cichonski et al.). NIST offers that such systems also increase time-to-restoration because they allow for synchronized efforts and increased collaboration (Cichonski et al.). The items that NIST recommends including during incident logging included significant items such as the incident's current status, early warning signs or indicators, Chain of custody, and the next steps to be taken to resolve the ongoing issue (Cichonski et al., 2012).

As the incident is being documented, incident handlers must notify the appropriate personnel to ensure that the incident is managed effectively. As discussed in previous chapters, there is a litany of individuals and organizations that must remain abreast of the ongoing incident depending on the threat and the systems impacted by the incident. NIST recommends that at a minimum, incident handlers must have defined procedures for reporting incidents (Cichonski et al.). These procedures should include a list of personnel, positions, and organizations to be contacted based on the incident in progress. NIST identified that common notification lists include chief information officers, information security professionals, internal and external incident response agencies, human resources, system owners, public affairs, legal, and law enforcement when necessary (Cichonski et al.). NIST recognizes that there are multiple technical platforms and applications available to streamline the notification process; however, NIST recommends the use of email, websites (portals), telephone, and in-person briefings (Cichonski et al.).

Incident notification is one area in which private industry and federal government research participants appear to have the largest procedural disparity. Multiple private industry participants (80%) indicated that their organizations are using automated processes and applications to notify technicians, IA professionals, organizational leadership, customers, and the authorities of ongoing incidents. This percentage of notification automation becomes more relevant as it was also identified that none of the federal government participants admitted to using automation in their respective incident notification processes. Multiple private industry participants (80%) were logging historical incident information and configuring their notification systems in a manner such that following an incident, the system would automatically generate a trouble ticket and based on the characteristics of the incident, the notification system would proceed to notify the appropriate technical agents, system owners, organizational leadership and external organizations. These automated logging and notification configurations almost certainly result in significant decreases in an organization's mean restoration timelines.

D. ORGANIZATIONAL INCIDENT CONTAINMENT, ERADICATION, AND RECOVERY

A good network incident containment strategy primarily provides two things: a limit on the spread to other network resources once an incident is validated, and additional time to implement the required eradication and resolution strategies (NIST, 2012). In either case, NIST emphasizes that an "essential part of containment is decision-making" and as such, decisions that affect adjacent business units cannot be made unilaterally within the IT department (NIST, pp. 35). In many cases, these decisions can be streamlined "if there are predetermined strategies and procedures for containing the incident" (NIST, 2012, p.35). However, the effects of an incident are rarely limited to just a single business unit, and in these cases, effective communication is key to efficient recovery.

1. Containment Strategy

Several research participants from academia and private industry discussed how leveraging communication platforms and workflow applications enhances communication between incident handlers and business unit leadership. Conversely, several participants from the federal government identified that these communications techniques were absent and noted that their primary source of initial incident information typically came from their local helpdesk. Within private industry and academia, all but two participating organizations tackled the business leadership integration problem through periodic strategy alignment meetings that took place with a daily, weekly, or monthly frequency. There were two primary instances where communication was continuous between incident management teams and business leadership. In both instances, the participant was a large private organization in the technology and cloud computing field. These two outlying private organizations took a different approach whereby leadership and subject matter experts from supported business units directly participated in the incident handling process through inclusion within the communication chain. In one case, a technology service provider chose to position business unit leadership and subject matter experts at key positions on the incident handling watch floor. While this level of involvement is not practical or even possible for all organizations and industries, the ease of communication

and unity of effort across business sectors expressed by those organizations that continuously included business leadership in the incident handling process was profound.

Contrary to what was observed in private industry and academia, participants within the federal government reported having trouble communicating with supported organization leadership. This was primarily due to the size and diversity of supported organizations and the hierarchical gap that separates incident handlers from those they support. In one case, incident management team leadership prioritized daily meetings with network management personnel acting as a mediator between IT personnel and organizational operations, though this was still limited by a rigid command structure. In another case, a government organization mentioned future efforts to develop and implement an exchange program between network managers from satellite network sectors to facilitate cross-training.

While both participants mentioned above are taking steps that resemble practices observed in the private industry, all government organizations identified a marked disconnect in communication between supported organizational leadership and supporting incident handling personnel. At best, incident management personnel relied on experiential knowledge of supported operations to understand service outage impact. At worst, service impact was only recognized after service interruption was in effect and the supported organization had engaged the helpdesk. The size and information sharing rigidity of federal government organizations certainly present unique challenges to communication and decision-making required in incident containment; however, the discrepancy between government and non-government participants was quite stark.

2. Evidence Gathering and Handling

In the process of troubleshooting and resolving an outage, incident handlers encounter and collect information that can be classified as evidence for future litigation should the cause of the outage be attributed to malicious intent. While incident management teams should remain cognizant that their actions and the data collected during the course of outage resolution may be used as evidence in a criminal investigation, NIST advises that they "generally stay focused on containment, eradication, and recovery" as

spending time conducting in-depth forensics "can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact" (2012, p.36-37). That being said, the desire to avoid task-creep among the incident handling team in no way abdicates them from detailed documentation practices. Instead, NIST makes the case that standard incident handling documentation practices should integrate evidence handling and forensic techniques as a matter of course, and is further outlined in NIST Special Publication 800–86, Guide to Integrating Forensic Techniques into Incident Response (2006).

Discussions on evidence gathering in the incident handling life cycle with participating organizations can be broken down into two major components: logging and interaction with law enforcement. The impact of network and system logs is typically determined long before an incident ever takes place and is closely tied to other phases in the incident handling life cycle as well as to higher-level policy decisions. Much of the specific recommendations for system logging are outlined in NIST's 800–53 and 800–92 Special Publications; however, the eradication and recovery phase of the incident handling life cycle is where sound logging policy decisions begin to bear fruit (NIST, 2020, 2006).

All participants identified having established system logging policy either at the local or enterprise level, although the policies for system log retention varied significantly from years to only a few months depending on the industry and customer requirements. Federal government organizations required the most robust long-term system logging policies, up to five years in some cases, due to U.S. federal government information control policies that are heavily influenced by the classification level of the system or network. The most prominent difference between private industry and government participants was the level at which system logs were maintained. In all private industry participants, system logs were collected and maintained at the same business unit level in which those systems were operated and maintained. This means that incident handlers assigned to a particular network segment have direct access to the logs for systems within that same segment. Conversely, only one federal government agency participant maintained and analyzed system logs at this local level. Instead, system logs were typically maintained at the enterprise level and required local system troubleshooters and incident handlers to request

logs for a system when required. Finally, in cases where a participating organization used autonomous or semi-autonomous monitoring tools, network trend analysis was conducted periodically or in real-time. However, once this system data was archived according to organizational policy, all participants mentioned that these archived logs were only accessed on an ad-hoc basis should they be required for evidence or some other legal action.

While there was some disparity between different industries in how logs are collected and maintained, there was a near consensus between all participants with regards to interaction with law enforcement. All participants interviewed identified that interactions with law enforcement and associated forensics analysis teams were as-needed once it became clear that criminal action was involved. All participants identified that incident handlers or in-house legal teams were authorized to pass criminal investigation and forensics procedures to local, state, or federal law enforcement as applicable. Only one private industry participant mentioned that it actively cultivated working relationships with law enforcement organizations in the form of invitations to audit network outage drills and war games. This same organization also mentioned membership to law enforcement-backed trade organizations to facilitate information sharing on malicious actors, zero-day vulnerabilities, and exploits observed across industry.

3. Eradication and Recovery

When it comes to network incident recovery, steps taken in previous stages of the incident handling process begin to pay dividends. In this stage, NIST identifies recovery actions such as "restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security" that can only be effectively accomplished because of prior decisions and actions (NIST, pp.37). Similarly, many of the actions and processes initiated in earlier stages of the incident handling life cycle are continued in this later stage. Practices like "higher levels of system logging or network monitoring" are initiated in earlier stages and continued into the recovery stage (NIST, pp.37). For this reason, much more emphasis should be given to the feedback loops depicted in the incident handling life cycle (Figure 1), rather than the linear layout of the individual stages.

Therefore, much of this section will highlight system prioritization and continuity of operations plans that are typically designed and implemented in the policy and preparation stages since eradication and recovery ideally involves the timely and accurate execution of those plans and the associated reporting required to improve those plans for future use (NIST).

All but one participant across private and government sectors indicated that they implement a continuity of operations plan and that the plan required testing at least on an annual basis. Exactly what was involved in each of these tests ranged broadly from annual continuity of operations meetings among business sectors to full scenario-based exercises and third-party penetration testing. However, only 16.6% of participating organizations mentioned doing any sort of large-scale incident handling drills or wargames with network incident handling personnel outside of periodic audits and penetration testing. Of the participants that were not conducting outage drills, many cited the fact that they were not willing to potentially interrupt live networks for the sake of training, and they did not find network simulation tools to be worth the expense.

All participants mentioned of the use of data backup and hardware redundancy solutions that were either implemented through redundant datacenters, cloud services, or on-site physical backups that can be leveraged to affect a recovery in the case of an outage. Of these three types of redundant systems, 23% of participants indicated they relied heavily on cloud technology and several others indicated a future transition to cloud solutions. Several participants (62%) also identified off-site backups or redundant datacenters, and finally only two participants mentioned they were heavily reliant on local backups in the case of a large-scale system restoration.

More telling was how the level of automation within an organization's restoration and service failover procedures correlated with the adoption of highly distributed cloud services that were either outsourced or operated directly by the participating organization. Of the 23% of participants that relied heavily on cloud-based backup and service failover solutions, all of them reported seamless or near-seamless (fifteen minutes or less) failover capabilities. Conversely, the remaining 77% of participants that used more traditionally managed redundant datacenters or local backups identified that failover required some sort

of intervention by network operations personnel though semi-autonomous, or fully manual means. As a result, restoration and failover in these semi-autonomous or manual systems was typically measured in hours rather than minutes. Additionally, the restoration timelines identified by those organizations that relied on contracted cloud services or off-site datacenter support were highly reliant on the service-level agreements associated with those systems and services. This fact further emphasizes the impact and role service-level agreements play in ensuring that restoration timelines meet customer and operational requirements, regardless of the technology implemented.

4. Post-Incident Activity

One of the most important stages of the incident handling life cycle, post-incident activities and reporting, is also the most frequently neglected. NIST emphasizes that upon completion of the restoration phase, "each incident response team should evolve to reflect new threats, improved technology, and lessons learned" (NIST, pp.38). The post-incident activity process includes post-incident meetings with business leadership and incident handling personnel, generation of reports from these meetings as well as the creation of a follow-up report outlining the details of the incident and the steps taken for recovery (NIST). NIST then recommends using the reports generated in the post-incident stage as training materials for new incident response personnel and as "a reference that can be used to assist in handling similar incidents" (pp. 39).

Many of the research participants alluded to incident handling documentation and lessons learned procedures as having increased institutional knowledge and assisted with the prevention of similar incidents in the future. However, the questionnaire developed for this research did not directly address post-incident activity and knowledge management procedures. This stage of the incident handling life cycle warrants further research. It is likely that the U.S. private industry has established effective post-incident activity measures that have applicability for implementation within defense enterprise networks. The researchers identified that multiple organizations from U.S. private industry have begun to implement varying levels of automation during the post-incident activity stage.

One example was identified in a recently released Amazon whitepaper (Amazon, 2021) on incident response. The whitepaper suggested incident handling teams could alleviate manual processes by automating steps in the post-incident activity stage (Amazon, 2021). Amazon offered that technicians can define the incident remediation pattern, decompose the pattern into actionable logic, and create code capable of performing that logic during future incidents (Amazon). This technology would result in decreased time to restoration and potentially eliminate incident handler alert fatigue (Amazon). Although this type of technology was not directly discussed during the research questionnaire, it reinforces the concept that the U.S. private industry is presenting incident handling use-cases worthy of federal government analysis and potential implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CONCLUSION AND RECOMMENDATIONS

The goal of this research was to identify applicable U.S. private industry incident management policies, tools, and procedures that could potentially enhance the resilience and availability of defense enterprise networks. The questionnaire developed and used for this research rendered several key findings among private industry and federal government participants. The most significant findings are categorized into five major themes that are summarized and explored further in the following sections: Policy implementation, SLAs, personnel training and certification, automation, and communication with organizational leadership. These major themes are coupled with associated recommendations that may be used by leadership and incident handling personnel alike to further improve the incident handling posture of defense enterprise networks. While the conclusions and recommendations below are focused on defense networks, they are in no way exhaustive and many apply to a wide range of industries and organization types. The researcher's recommendations are not intended to undermine the credibility of defense incident handling teams or to suggest that these changes alone would result in a fully functional incident handling capability. Instead, the recommendations below serve as a starting point for future growth within the defense network paradigm, as a key observation throughout this research was the relative success experienced by organizations that constantly sought intentional and introspective improvement through learning, research, and a willingness to adapt and change to new technologies and environments.

A. POLICY ADOPTION, IMPLEMENTATION, AND DISSEMINATION

Based on the research analysis, NIST's Incident Handling Guide is clearly being leveraged across multiple industries by organizations ranging in size and responsibility. This prolific use appears to be because NIST provides incident handling teams with baseline procedural recommendations for each stage of the incident handling life cycle and allows organizations to deviate based on individual use case. NIST's Incident Handling Guide is not an all-encompassing, rigid plan that impedes personalization. All research participants that used NIST frameworks admitted to deviating from NIST's Incident

Handling Guide in some capacity; however, deviations were nearly always additive response measures that built upon NIST policy and not a complete departure from the guide's recommendations.

There were organizational disparities that became evident when analyzing private industry incident response methodology when compared to their counterparts in the U.S. federal government. Within government organizations, a large portion of incident handlers interviewed lacked conceptual understanding of how their respective organization's incident handling policies related to federal policy and NIST's incident handling framework. Incident handlers from less than half (40%) of the participating government organizations acknowledged that they understood the procedural requirements necessary to execute their daily job responsibilities but did not know if their organization's incident handling procedures were derived from federal or local policies and directives. This was in contrast to what was seen in private industry and academia where organizational policy and frameworks were well known among incident handlers.

Regardless of the framework or compliment of frameworks chosen for implementation on defense enterprise networks, if personnel tasked with handling outages are unfamiliar with the framework and its intent, any policy decisions made at higher echelons are irrelevant. Whether NIST, ITIL, or another incident handling framework, the researchers recommend that it should be clear at all levels what framework is being used and why. Public law and policy are not only complicated, but within a highly hierarchical organization such as the DOD, those policies and law become progressively more convoluted as they trickle through multiple levels of bureaucracy and layers of local policy are added during dissemination. This makes comprehensive understanding of applicable policy and associated legal documents produced across the entirety of the organization difficult to obtain. Also, incident handling personnel typically lack the time necessary to develop an understanding of public policy at this level. However, it is not unreasonable for incident handling personnel to have a working knowledge of foundational frameworks from which their standard operating procedures are derived. In fact, the DOD has a model for this type of documentation chain and standardization.

The Navy and Marine Corps aviation communities have a slew of governing publications that dictate everything from the legal requirements of operating an aircraft in civilian airspace to employment tactics in non-permissive combat environments. Each of these documents is rooted in complex layers of policy and doctrine; however, the publications referenced by the aircrew are written specifically to be read from the perspective of the operator. Each of these documents directly references governing policy documents from which they derive their authority and the Commander of Naval Air Forces (CNAF) has implemented the Naval Air Training and Operating Procedures Standardization (NATOPS) program as a check to ensure continuity and compliance among operators (i.e., aircrew), local standard operating procedures, and policies at the service branch level.

Similarly, the researchers recommend service-level publications and standardization programs should be implemented for incident handling personnel to distill the substantial body of policy and procedure into operationally practical and organizationally auditable manuals that are derived directly from, and reference, established DOD policy. Additionally, the DOD should consider implementing joint or service branch level audit and standardization programs that control and disseminate changes to incident handling manuals, as well as audit local organizational policy and SOPs for compliance and implementation. This standardization agency should carry out inspections annually and be cognizant of systems and use cases that may be unique to certain organizations based on mission requirements. Equally as important, any centralized standardization body should provide a simple means for incident handlers to suggest changes to manuals and procedures based on what operators are seeing at the local level. Bottom-up learning and growth should be encouraged just as much as top-down standardization if the DOD is to remain agile and relevant. Having a centralized standardization body allows for bottom-up feedback to be quickly incorporated into official procedure and widely disseminated. This type of system can only be effective if it exists to serve the incident handling personnel at the local level and provide practical and easily digestible products. Additional levels of oversight with no other purpose will only add ambiguity and bureaucracy. The main purpose should be to establish the foundation of

what will eventually lead to a formalized community of practice that enhances and preserves the institutional knowledge of incident handlers across the DOD.

In summary, organizational leadership should consider:

- Committing to an incident handling policy and framework that applies to their needs and use-case and ensuring it is clearly communicated at all levels.
- Establishing a standardization body to develop and disseminate practical and digestible tactics, techniques, and procedures publications to be used as a foundation for all incident handlers.
- Establishing an annual inspection program to ensure compliance and standardization among subordinate organizations that can be adapted for any system and mission that may be unique to individual subordinate organizations.

B. SERVICE LEVEL AGREEMENTS

All participants identified the importance of SLAs in policy implementation due to the role and impact they have on network incident response. Therefore, they cannot be ignored during the planning, implementation, or execution of the incident handling process. The creation of effective SLAs presents a difficult challenge for incident management personnel and organizational leadership because the terms of SLAs are typically decided years prior to implementation during the request for proposal (RFP) process. In the past, these decisions have excluded input from the incident management professionals responsible for carrying out the gamut of incident management responsibilities. Every research participant emphasized the critical role SLAs play in daily incident management operations; hence, incident handlers must develop an understanding of the details included in their respective organization's contractual agreements. In general, the DOD's hierarchal structure makes it easy for SLAs to become disjointed and misunderstood by incident handling teams attempting to troubleshoot contractually supported systems and services when compared to less complex organizations. The lines that subdivide areas of responsibility between incident handling teams and contractors can easily become unclear, leading to bottlenecks and longer resolution times. This issue will become increasingly

relevant as more services are outsourced or contracted in the DOD's push for growth in cloud technologies and as-a-service paradigms.

Fortunately, the issues surrounding SLA integration and mutual understanding of their terms by incident handlers and contracted support are closely related to the realm of policy implementation, and therefore can be similarly resolved. Just as public law, regulation, and high-level policy should be distilled down for practical understanding by incident handlers at the local level, SLAs should also be incorporated into local orders and daily incident handling tactics, techniques, and procedures (TTPs). Additionally, systems should be put in place to ensure that when contracts involving SLAs relevant to incident handlers are introduced or updated, the local policy and procedure manuals can be efficiently updated and controlled for accuracy. This duty should also fall onto the standards organization mentioned earlier, which should already be tasked with creating, and updating incident handling TTPs and manuals. Standards organizations can also act as intermediaries between contracted support and incident handling personnel. Finally, given the recommendation in the previous section that a standards organization should be responsible for soliciting and integrating suggestions for changes to TTPs, this same standards organization could also collect issues and suggestions concerning the terms in SLAs from incident handlers and relay them to contract writers for incorporation into future contracts within the DOD.

Ultimately, it is imperative that all entities affected by a given SLA are familiar with the SLA terms and procedural applicability to avoid potential friction when in the process of handling an incident. It is either the priority or responsibility of incident handling personnel to decipher the intricacies of a given SLA involving contracted support while attempting to resolve an incident. Therefore, it is imperative that organizational leadership implement policy and safeguards that make interactions between incident handling teams and contracted support as seamless and unambiguous as possible.

In summary, organizational leadership should consider:

- Ensuring the details of SLAs and applicable contracts are incorporated in local orders, incident handling TTPs, and operating manuals in an easily digestible and practical way.

- Providing a process for disseminating, updating, and inspecting the applicable details of SLA incorporation into local orders, incident handling TTPs, and operating manuals.

- Establishing an easily accessed entity to act as an intermediary between incident handlers and contracted support in the case that areas of responsibility should be unclear to either party.

- Establishing an easily accessed entity to solicit, collect, and convey feedback and suggestions about SLA terms and incorporation from incident handling personnel and contracted support for use in future contracts and SLAs.

C. INCIDENT HANDLING PERSONNEL TRAINING AND CERTIFICATION

On several occasions during the research, participants identified the difficulty that incident handling team leadership had in determining appropriate training, certification, and qualification requirements for incoming applicants or new servicemembers for a given position. Participants from the U.S. federal government especially, identified a reliance on an outdated certification model to measure the ability of a servicemember to take on upper-level roles and responsibilities. Participants from both the U.S. private industry and the U.S. federal government agreed that static third-party certifications and advanced degrees have become increasingly less relevant in the constantly shifting technological environment for assessing the practical competency of an applicant. As technology and network security threats rapidly evolve, private industry participants were adamant that first-hand experience serves as the best measure of performance potential when assessing a new hire. The lack of comprehensive, effective training pipelines and solidified training requirements has resulted in subjective hiring qualification requirements within private industry and an ineffective career progression model within the DOD. These subjective

hiring and continuing education models result in organizational limitations and make it difficult for incident handlers to transition between varying sub-units within an organization. Skills and individual abilities prioritized by one incident handling team may not overlap with another, especially as processes and procedures appear to vary within the government's distributed team construct. It is vital that the U.S. federal government establish an updated policy that details achievable, preliminary incident handling training, emphasizes experience, and breaks away from rigid certification requirements.

Although an applicant's abilities upon hiring are important, continued training and education are critical components to ensure the growth of an incident handler. An organization's long-term training initiatives are responsible for enhancing the effectiveness of the incident handling team and should evolve with the threat over time. Participants from private industry and federal government offered that annual training plans were difficult to formalize and real-world exercises on live networks were too risky. These factors resulted in over-reliance on certifications and on the job training (OJT). While third party certifications and OJT can reinforce basic concepts and serve as mechanisms for continuing education, they should not be the only instruments for training incident handling professionals. Training on test networks or ideally live organizational networks should be incorporated in an attempt to mimic real-world incident response. The risk of potentially degrading a non-critical service during low-traffic hours would be significantly outweighed by the vital training an incident handler would receive as a result of training on the actual systems, applications, and network that they monitor on a daily basis. Organizations can overcome the risk of a potential outage by scheduling authorized service interruptions (ASIs) during the period of training which would inform their users of a potential outage. However, the likelihood of an outage being caused by incident handling training on the live network would be minimal as most incident handlers do not have the network permissions necessary to make configuration changes necessary to cause a widespread network outage.

Many of these changes to training paradigms can be fixed using tools already well known to DOD organizations, and would simply require the application and reinforcement of these organic training models. Training and qualification standards models already exist

within the DOD, such as the Marine Corps' Training and Readiness (T&R) model and the Navy's Personnel Qualification Standards (PQS). These training regimens outline step-by-step standardized education and apprenticeship pathways for personnel to follow in the course of their career progression. T&R manuals define everything from formal education requirements, classroom study and OTJ, to practical evaluations and competency-based examinations. All with the purpose of standardizing the training and qualification requirements for specific occupational specialties across the force. It may be beneficial to develop a similar T&R pipeline and associated manual for incident handling personnel. Like the T&R programs for other occupational specialties, the training and qualification requirements for the entirety of a defense incident handler's career should be laid out in an incremental format that is implemented regardless of geographic or combatant command. Care should be taken to ensure that these training requirements are as technology-agnostic as possible to provide the widest applicability. This would be accomplished by focusing on conceptual mastery evaluated by senior incident handlers, similar to the scenario-based qualification board concepts used in the surface, subsurface, and aviation warfare communities. Additionally, the introduction of a standards organization mentioned in previous sections could ensure that these training requirements are updated regularly to reflect changes in policy and procedure as well as provide graduate-level courses for incident handlers to become resident experts and senior-level instructors within their local units, similar to the function of weapons schools implemented in other communities. These training standards and pipelines need not be developed entirely in-house, and it is certainly reasonable that qualifications outlined in T&R manuals be directly correlated to certifications developed in the private industry. However, the desired end-state of this T&R system should be that new and experienced incident handling personnel have a clear understanding of both short-term and long-term training and career progression pipelines, and that incident handlers have their education seamlessly continued and qualifications recognized as they transition between organizations within the DOD.

In summary, organizational leadership should consider:

- Replacing rigid third-party certification guidelines resident in the DOD 8570 training manual with new training guidelines that detail the specific and standardized job experience outlined in digestible T&R manuals.

- Accepting the risk associated with training incident handlers on live networks. Leadership should mitigate the risk by conducting incident handler live training during low-traffic hours and scheduling ASIs to coincide with potential services outages that may be created by the training.

- Creating qualification programs evaluated on conceptual and scenario-based mastery that are standardized across the force where progression can continue through personnel transitions.

- Creating a training standards organization responsible for updating training and qualification standards and manuals and to act as a graduate-level school producing resident experts and senior-level instructors for local organizations.

D. AUTOMATION

An important theme identified during the research was the automation of incident monitoring, notification, and response processes. Each research participant from private industry and academia included elements of automation during at least one stage of the incident handling life cycle, while participants from the federal government were either still in the process of transitioning to automated incident handling practices or planning future implementation. During the preparation stage, several organizations from private industry had developed robust self-help or TIER 0 troubleshooting portals and applications for their users. One participant from the private industry explained that many of their TIER 0 incidents, including password resets and software downloads, are being resolved directly by users interacting with an automated system. Automated TIER 0 support enabled incident handling personnel to focus on troubleshooting significant issues and threats impacting their networks. Future quantitative research that evaluates the impact that automated helpdesks have on the overall reduction of time-to-restoration may have practical use in the incident handling domain.

During the detection and analysis stage, active and passive network monitoring tools and applications are being implemented by nearly all participants from private industry and academia. This capability enables the automated monitoring of networks, systems, and business applications. Private industry has configured network devices and business applications in a manner that automatically alerts technicians when device or application suites are degraded or offline. Private industry participants also implement proprietary software or commercial off-the-shelf solutions from ServiceNow, PagerDuty, and Splunk that automatically detect anomalous activity, service degradation, and equipment outages. These tools automatically create trouble-tickets which detailed pertinent information about incidents and simultaneously notify technicians responsible for troubleshooting by email, telephone, and chat application. By automating the workflow process to include documentation, trouble-ticket creation, and notification, these tools save organizations a significant amount of time during the early stages of the incident handling process.

During the containment, eradication, and recovery stage multiple private organizations had configured their networks redundantly, allowing for seamless failover capabilities when incidents did arise. Multiple private organizations had also configured their software to automatically contain or quarantine portions of their network when anomalous activity was detected. This capability provided security and incident handling professionals the time needed to perform an initial diagnosis, confirm the threat or outage, troubleshoot, and eradicate the issue. Conversely, several research participants from government organizations admitted that the majority of their incidents were being initially identified by users. This phenomenon resulted in a reactive vice proactive incident response posture that lead to a piling-up of restoration tasks in incident handling workflows. During the post-incident activity stage, many research participants from the private industry advocated for open lines of communication between the U.S. Government, law enforcement, and other incident response organizations. These participants suggested that effective information sharing relationships often resulted in robust lessons-learned archives. Lessons learned, when used effectively, can aid systems and network engineers in developing future network configurations that automatically prevent threats or restore

services that have been regularly experienced in the past. As explained in NIST's Incident Handling Guide, incidents are not completely preventable; however, organizations must learn from past incidents, identify reasons for a given outage, and manage their network to prevent similar outages in the future.

In summary, incident handling teams should consider:

- Leveraging automated helpdesk technologies to include commercial-off-the-shelf customer relationship management tools that autonomously reconcile common helpdesk functions.

- Implementing commercial off-the-shelf automated workflow solutions that proactively identify incidents, document incident details, create trouble-tickets, and notify incident handling personnel of the ongoing event.

- Prioritizing lessons-learned documentation and information sharing that details threats, outages, and degradations for incorporation into planning efforts with systems and network engineers to prevent like-incidents in the future.

E. COMMUNICATION WITH ORGANIZATIONAL LEADERSHIP

The researchers identified a large disparity amongst U.S. private industry and federal government participants when it came to existing interaction and support from organizational leadership. Private industry participants emphasized the importance of communication between incident handling teams and organizational leadership in the form of regularly scheduled meetings, debriefs, and exercises. Several private industry participants had strategically placed incident handlers inside individual business units to serve as direct liaisons between the organization's coordinating incident handling team and each business unit.

Conversely, participants from the federal government admitted that open communication between incident handling teams and organizational leadership was lacking. Terms such as "unacceptable" and "requiring immense improvement" were used to describe this relationship. Without effective top-down and bottom-up interaction and regularly scheduled communication between executive leadership and incident handling

teams, organizational goals and strategy can quickly become disjointed and incoherent. Incident handlers from multiple organizations that support defense enterprise networks recognized that they had a limited understanding of critical organizational policies and the underlying missions they supported. One participant offered that executive leadership only became interested when significant issued appeared. This lack of cohesiveness can negatively impact the accuracy, prioritization, and categorization of outages and service degradations due a mission purpose mismatch. When incident handlers don't anticipate the impact network systems and services have on real-world operations, the likelihood of handling an incident in a way that effectively supports overall mission success is unlikely.

Executive leadership should continuously communicate with incident handling teams to refine system prioritization and incident categorization. These priorities change over time as new technologies and strategies are introduced. NIST emphasizes the importance of communication between business leadership and incident handling teams in maintaining unity of effort for the sake of mission success. Executive buy-in and support is necessary for incident handling teams to create effective incident handling policies that are widely accepted and accurately enable supported operations within an organization (Cichonski et al., 2012).

In summary, organizational leadership should consider:

- Introducing at a minimum, a weekly meeting that includes members of the executive leadership team and the incident handling team.
- Placing an incident handler within each critical business unit to serve as a liaison between business unit leadership and the organization's coordinating incident handling team.
- Developing a policy to document and debrief high priority incidents that includes executive leadership in the dissemination of those debriefs.
- Conducting semi-annual table-top exercises involving executive leadership and incident handling teams to validate incident response policy and procedure. These exercises should account for supported operations and realistic mission objectives.

Although this research has developed several key conclusions and recommendations for implementation within the incident handling community, it should be noted that the research model had several key limitations that may have impacted the suggestions made by the researchers. The research sample was limited in size to only thirteen participants and included only a small subset of industries. While the response from each organization was comprehensive, in some instances including executive leadership, a larger sample size would provide a better representation of the incident handling community. Additionally, while the questionnaire was modeled after the recommendations established in NIST's incident handling guide, future research that focuses on an analysis of the post-incident activity stage of the incident handling life cycle would better serve to improve the understanding of the lessons learned process. Further research of post-incident activity could potentially aid internal and external information sharing, as well as in the development of a lessons learned collection and dissemination policy. Finally, the researchers focused more on the policy and processes that make up the incident handling life cycle and less on the new technologies that have reinvented these processes over the last decade. Future research that analyzes specific technologies available to incident handlers and the effect each system and service has on quantitative restoration metrics would also benefit the incident handling community.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. RESEARCH QUESTIONNAIRE

Institution:			
Version:	3.3.1 - 09OCT2020	**Date:**	

The following questions are centered around the network and enterprise architecture of your organization, as well as the tools, policies, and procedures used to detect, identify, and resolve network outages of all types. In addition to questions about the network itself, we will also be asking questions about how your organization's core services and business strategy dictate those network policies and procedures. The classification level of this research is unclassified and open distribution. Please do not give any classified or FOUO information in your responses. There will not be any personal questions or personally identifiable information collected in the process of this interview, participation is completely voluntary and can be retracted at any time.

	Section 1: Policy, Methodologies, Structure, and Standards
1.1	Are network or network segments required to adhere to policies, regulations, or standards that are imposed by an external agency or organization?
1.2	Do network or network segments voluntarily adhere to the policies, regulations, or standards of an external agency or organization?
1.3	Are network diagrams maintained that represent the digital and physical network architecture?
1.4	Are unclassified network diagrams available for our analysis?
1.5	If the classification level of network diagrams is designated FOUO, can the high-level network topology be described instead?
1.6	What operational or user requirements and constraints drove the decision to use the aforementioned topologies?
1.7	Which segments of your network maintain consistent direct contact with cloud-based assets or services?
1.8	What business objectives lead to the implementation of cloud-based assets or services?
1.9	What network management protocols, quality of service protocols, and/or support services are currently used?

Section 1 (Continued): Policy, Methodologies, Structure, and Standards	
1.10	What network or user requirements constraints drove the decision to use the aforementioned network management protocols, quality of service protocols, and/or support services?
1.11	Are network-related resources, services, or applications outsourced to a contracted agency?
1.12	How do incident response policies and protocols differ for incidents that involve contracted or vendor support?
1.13	Under what conditions would internal incident response personnel interact with vendor support during incident response?
Section 2: Personnel, Training, and Network Operations Center Structure	
2.1	What are the reporting chains of command within the Network Operations Center, and can an organization chart be provided?
2.2	How many technicians are employed within the Network Operations Center?
2.3	Are all Network Operations Center technicians physically located in one area or are they geographically distributed?
2.4	Are there specialists or external contractors employed to work on or aid in the management of the network?
2.5	If so, are these contractors physically located within the Network Operations Center?
2.6	What formal certifications are Network Operations Center technicians required to achieve and maintain?
2.7	What approach is used to optimize communication with external and cloud service providers?

Section 2 (Continued): Personnel, Training, and Network Operations Center Structure	
2.8	Is there a standardized on-the-job training plan for technicians outside of formal certifications?
2.9	What type and how frequently are network outage drills or scenario-based training conducted within the Network Operations Center (penetration testing, natural disasters)?
2.10	What type and how frequently do non-IT personnel receive training concerning network use and policies?
2.11	What business units and/or business functions are supported by your Network Operations Center environments and technicians?
2.12	What standard service agreements or offerings exist that specify Network Operations Center availability and/or recovery requirements?
2.13	Is a helpdesk employed within, or directly associated with the Network Operations Center?
2.14	Is the Network Operations Center helpdesk centralized or disaggregate across network sectors?
2.15	What policies, procedures, or restrictions dictate the physical layout of the Network Operations Center floor?
2.16	What policies, procedures, or restrictions dictate the sections/support domains that exist within your Network Operations Center physically/logically?
Section 3: Incident Identification Tools and Procedures	
3.1	What types of enterprise events, systems, and applications are actively monitored at the network level?
3.2	What types of enterprise events, systems, and applications are passively monitored at the network level?

Section 3 (Continued): Incident Identification Tools and Procedures	
3.3	What network monitoring and incident management tools are used to conduct this monitoring?
3.4	What types of alerts or notifications are used to alert personnel of an incident?
3.5	Who receives these notifications?
3.6	Describe the network logging policy (what gets logged, how those logs are stored and how long they are kept, etc.).
3.7	What are the policies in place for incident categorization, scoring, and prioritization?
3.8	What critical core services are supported by the Network Operations Center?
3.9	Are there different restoration timelines associated with specific core and/or priority services?
3.10	Describe the Continuity of Operations Plan (COOP)?
3.11	What tools and technology-implemented policies are being used to back up core-service critical data in the event of a loss?
3.12	What network hardware and data center redundancies are readily available and/or active in the event of a loss?
3.13	What policies are in place to notify and disseminate information about the adverse event to other networks within the Enterprise?

Section 3 (Continued): Incident Identification Tools and Procedures	
3.14	What is the response protocol for an incident that requires contracted or vendor support?
3.15	What are the policies and procedures for involving law enforcement in the case of a malicious event?
Section 4: Program Management Techniques	
4.1	How does the Network Operations Team leadership work with business leadership to align network operations to business objectives?
4.2	How does the organization's business strategy determine particular network service priorities?
4.3	Do the members of the Network Operations Center maintain certifications in program management methodologies (e.g. PMP, Lean 6 Sigma Belts).
4.4	What project management methodologies are used to manage major updates or technology transformations (e.g. Waterfall, Agile approaches)?
4.5	What techniques are used to ensure continuity of service during major updates or technology transformations?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agutter, C. (2019). *ITIL® foundation essentials - ITIL 4 Edition: The ultimate revision guide* (2nd ed.). IT Governance Publishing.

Amazon. (2021). AWS security incident response guide. AWS Technical Guide. Retrieved from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.pdf#automating-incident-response

Chandersekaran C.S., & Simpson W.R. (2011) A multi-tiered approach to enterprise support services. In A. Marcus A. (Ed.) *Design, user experience, and usability. Theory, methods, tools and practice. DUXU 2011*. Lecture Notes in Computer Science, vol 6769. Springer, Berlin.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., (2012). *computer security incident handling guide*. (Special Publication 800–61). The National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

E-Government Act of 2002, Pub. L. No. 107–347 § 116 Stat. 2899 (2002). https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283 § 128 Stat. 3073 (2014). https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T., (2006). *Guide to test, training, and exercise programs for IT plans and capabilities*. (Special Publication 800–84). The National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-84

Grimes, J., (2005). *Information assurance workforce improvement program*. (DOD 8570.01-M). Department of Defense. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

Lichtenthaler, U. (2018). The world's most innovative companies: A meta-ranking. *Journal of Strategy and Management, 11*, 497–511. https://doi.org/10.1108/JSMA-07-2018-0065

National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations* (Special Publication 800–37). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations*. (Special Publication 800–53). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Office of Management and Budget. (2016). managing information as a strategic resource (Circular No. A-130 Revised). https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

White House. (2017). *National security strategy of the United States of America.* https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California