[redacted]

(1)

Report Number XX-XX

# (U) Integrating Network Risk Analysis Methodologies into Command and Control, Battle Management Communications (C2BMC) System Test, Evaluation, Exercise and Experimentation

[redacted]

Classified By: Multiple Sources (Sources listed in Appendix A)

Classified On: 11 July 2013

Declassify on: Manual Review

[redacted]

DISTRIBUTION STATEMENT C

Distribution authorized to U.S. Government Agencies and their contractors; administrative or operational use; 11 July 2013. Other requests for this document must be referred to USSTRATCOM/J81 or higher DoD authority.

[redacted]

[redacted]

(U) Contents

# 1 (U) Executive Summary

(U) This document is an initial cyber vulnerability assessment for the Command and Control, Battle Management and Communications (C2BMC) system with the objective of providing a foundation on which more detailed and focused assessments might be made in the near future. These future assessments would employ Integrated Ballistic Missile Defense (IBMD) and C2BMC subject matter experts (SMEs) to help refine and specify much of the information articulated in this report. This assessment report is the product of Ballistic Missile Defense System (BMDS), C2BMC, and cyber threat document reviews conducted by cyber security SMEs using Department of Defense (DoD) accredited Network Risk Assessment Tool (NRAT) methodologies. The report is focused on cyber threats to the C2BMC system and does not include potential threats to peripheral systems within the BMDS infrastructure. Similarly, threat mitigation or contingency plans which use peripheral systems during a cyber attack are not considered in this report.

[redacted] The preliminary analysis conducted using the NRAT methodology provides some insight into the operational risk from exploitation or attack of the C2BMC system. [redacted] (b)(1) [redacted] While the overall BMDS may have [redacted] (b)(1) [redacted] C2BMC system, the intent of this report is to identify realistic threats with the potential for operational impact on C2BMC supported missions.

[redacted] This report sets the stage for more detailed, follow-on analysis that will provide more detailed answers for exercise scoping and refines direction toward cyber threat awareness and risk mitigation for the C2BMC system. Because the content of this report is the product of analysis of limited, published C2BMC and BMDS documentation reviewed by cyber security experts, the report concludes with recommendations for subsequent analysis using the NRAT capability with BMDS operators and planners in an experiment or exercise environment.

# 2 (U) Introduction and Background

[redacted] The Director, Operational Test and Evaluation (DOT&E) is responsible for ensuring deployed systems undergo realistic testing with opposing forces (OPFOR) representing real-world capable threats in an operationally representative environment. [redacted] (b)(1) [redacted] Range events have traditionally been used to provide testing environments without affecting operational systems. While a range environment enables recreation of technical aspects of cyberspace, it can be difficult to scale the environment to the level of the interconnectivity provided by wide area networks and interoperability with infrastructure not provided by the system under test (SUT).

[redacted] (b)(1) [redacted] DOT&E has been working to [redacted] (b)(1) [redacted] live, virtual, and constructive (LVC) range environments to present more realism in the

environment and development of red team capabilities to be presented in a more representative OPFOR during the events.

[redacted] To aid in identification of threat portrayal and test objectives, it is useful to conduct analysis of a SUT prior to the event to identify most likely and most impactful threat actions associated with threat actors of concern. This helps to set initial boundaries for the event and identify data collection opportunities prior to execution in order to gather empirical evidence of cause and effect relationships which will support post-event analysis. One approach to examine red-on-blue events is to examine operational risk imposed by the threat of exploitation and attack of information systems supporting operations. The Network Risk Assessment Tool (NRAT) was established to conduct such an analysis in a structured and repeatable manner. It has been utilized for numerous studies including but not limited to command and control systems for U.S. Pacific Command (USPACOM), cyber threats to space networks, and network vulnerability studies for systems which support Nuclear Command and Control (NC2). The methodology and operational tool has been Tri-Service reviewed and approved.

(U) One of many critical missions relying heavily on cyberspace capabilities is that of Ballistic Missile Defense (BMD) in the rapid identification, characterization, and sharing of BMD threats. A key portion of the BMD mission system is the C2BMC.

(U) This report provides an initial risk assessment of the cyber threats which could potentially affect the C2BMC system. Additionally, this report builds upon BMD cyber vulnerability studies that have been conducted over the last several years by the National Air and Space Intelligence Center (NASIC), Defense Intelligence Agency (DIA), National Security Agency (NSA), U.S. Strategic Command (USSTRATCOM), and various Service Information Operations (IO) commands. Appendix A provides a list of references for these studies.

[redacted] For this report, the cyber vulnerability assessment methodology underlying the Network Risk Analysis Tool (NRAT) is applied to the C2BMC system based on published documentation and interviews with BMD experts. Therefore, this report delivers an initial assessment by cybersecurity analysts without direct BMD expertise. Accordingly, the objective of this assessment is to provide a "first look" at potential C2BMC cyber vulnerabilities and recommendations to employ the full NRAT capability with BMD subject matter experts (SMEs) in order to deliver more specific and detailed analysis in future experiments or exercises.

## 3 (U) Assumptions and Limitations

[redacted] This study is intended to focus solely on a single C2BMC suite. It is understood that C2BMC is part of a system-of-systems architecture for the larger BMDS, yet by focusing on C2BMC it is possible to obtain additional detail and more fully understand aspects of cyber threats to the operation of this portion of the BMDS system. This assumption should be carefully considered in context of the larger BMDS system before conclusions are drawn about true risks to the overall system. But understanding how a portion of the BMDS can be affected by credible and plausible cyber threats can be crucial to

crafting new architectures or tactics, techniques, and procedures (TTPs) to handle non-standard system behavior and maintain mission readiness for the overall BMDS.

(U//FOUO) A limitation of the study is that the methodology inputs were derived from information available through searches of the Secure Internet Protocol Routed Network (SIPRNET) available websites and limited interviews with personnel familiar with BMDS and C2BMC. The inputs used in the analysis need to be updated with SME validated data for each aspect of the methodology.

# 4 (U) NRAT Methodology Overview

(U//FOUO) NRAT is a high level analytical tool used for evaluating operational risk from cyber threat actions against supporting information systems. The methodology uses a probabilistic risk analysis framework to provide a rating that correlates with the relative likelihood of a threat action being successfully perpetrated against a particular information system. This rating is based on the capabilities and intent of potential threat actors, the effect mechanisms of the threat action, and the vulnerabilities of the targeted information system; in this case, C2BMC.

(U//FOUO) As an operational risk assessment tool, NRAT considers two fundamental risk components: the likelihood of a cyber attack occurring and the severity of that attack on the missions or operations supported by the information system under attack. NRAT considers the likelihood of a cyber attack by evaluating two questions: 1) Is there an actor that can competently execute the threat action? And 2) Is the target information system vulnerable to that threat action? For the severity of attack success, impact assessments are assigned from the attack influences on services and data provided by the information system followed by an impact assessment to the missions following a loss of service or data security. Figure 1 below illustrates the general framework used to compute likelihood and severity to assess the operational risk. Refer to the NRAT Analyst Manual for detailed explanation of the underlying methodology.[1]

[1] USSTRATCOM J86 (2010). *Network Risk Assessment Tool (NRAT) Analyst's Manual for App Ver. 3.3 Revision 0*

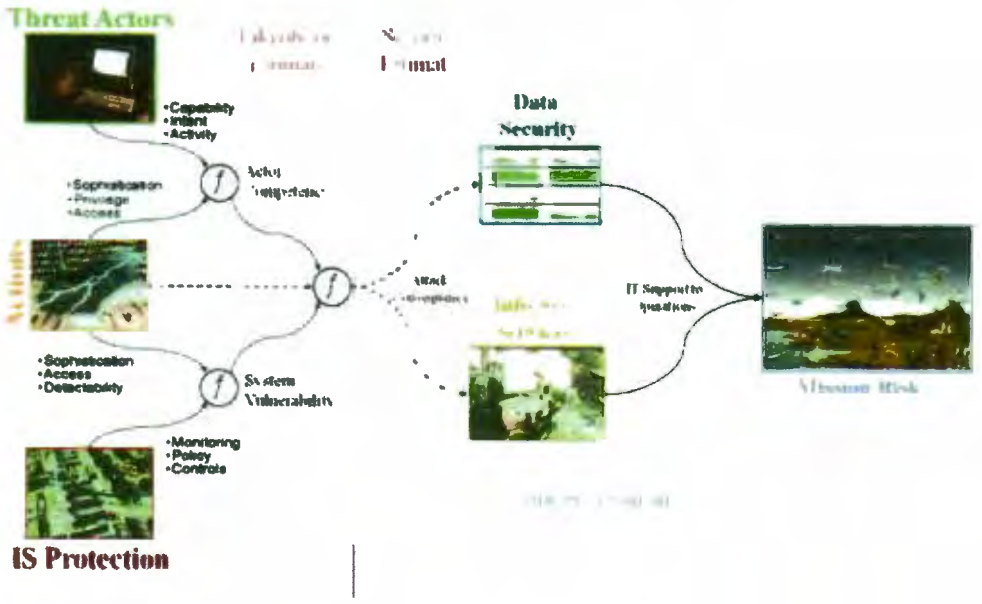



*Figure 1 (U) NRAT Risk Assessment Framework*

## 5 (U) C2BMC System[2]

(U) C2BMC is the integrating element of the BMDS that connects sensors with shooters. The capability provides the users with a suite of tools to plan, monitor, execute, and communicate BMDS plans and actions. Specifically, C2BMC enables users to build plans which allow the warfighter to assess BMD courses of action. C2BMC also provides a common situational awareness (SA) picture for operators and senior leadership who must interoperate among coalition and allied forces. Additionally, the capability provides battle management tools, like Global Engagement Management (GEM), which allow users to rapidly analyze, coordinate and remotely execute missile defense via multiple, world-wide sensors for optimal defense coverage. In order to perform these functions, C2BMC provides global connectivity between BMD assets by linking solutions to get the right data to the right asset using the DoD network infrastructure.

(U) As the integrating element of the BMDS, C2BMC connects sensors, weapons, and fire control assets into a global network. The Command and Control (C2) function provides hardware and software to plan integrated missile defense (IMD) operations and delivers SA data through a series of maps, tracks and tables in a common operating picture (COP) format. This COP displays the global BMDS elements' Operational Capability (OPSCAP) and Health and Status (H&S) information.

(U) The Battle Management (BM) function includes the monitoring and assessing of enemy activities while also planning and controlling future and current operations. The function provides SA of the

[2] (U) Missile Defense Agency (2012). *Ballistic Missile Defense System Handbook (S)*. Author

employment of IMD sensors and shooters; track management of BMD track reports; and monitoring of the engagement status of BMD sensors and weapons.

(U) The Communications function of C2BMC establishes and maintains the BMD network for the protected exchange of data including integration with various sensor and shooter communication systems.

(b)(1)

(U) Because the C2BMC functions rely heavily on a complex information system infrastructure that includes cross domain transfer of secure information and the global transmission of sensitive data, there is significant risk to BMD information confidentiality, integrity and availability. The following section describes possible threat actions and provides an assessment for attacks which could exploit existing vulnerabilities in the C2BMC information system architecture and impact the BMD mission.

## 5.1 (U) Missions

(U) The NRAT methodology focuses on presenting risk in an operational context that is relevant to the Commander's overall responsibilities. In order to analyze operational impact, a list of missions or operational tasks is developed that is supported by the system under evaluation. For the case of C2BMC, these missions were derived from documentation of the operational tasks or objectives supported by the system.

*Table 1 (U) C2BMC Mission List*

| C2BMC Supported Mission | Description |
|---|---|
| BMD Planning | Conduct tasks such as sensor tasking, engagement resource allocation, and logistics support. This includes deliberate and dynamic planning, coordinating, preparing for, and sustaining BMD operations. |
| BMD Asset Monitoring | Monitoring of asset status information to present a common SA picture for operators and senior leadership including the delivery of enemy and friendly SA data through maps, track and tables via a COP. Specifically, enemy activities are assessed in coordination with friendly force maneuvers. |
| BMD Execution | Conduct of sensor tasking, threat data fusing, and execution of capabilities to engage a threat. Provides SA of employment of sensors and shooters, track management, and intercept engagement. |
| BMD Communications | Provide global connectivity between assets, planners, and operators. Establishes and maintains BMD communication network (BCN) for secure data exchange among BMD elements. This includes integration with numerous sensor and shooter communication systems and their associated formats and protocols. |

## 5.2 (U) Information Services

(U) Information services are those functions or capabilities provided by C2BMC to the operators and users to support missions stated in 5.1 above. As illustrated in Figure 1 above, missions are supported

and thus impacted given a loss of information services or security of data processed or stored on C2BMC. The following is the list of information services and data sets provided to operators by C2BMC.

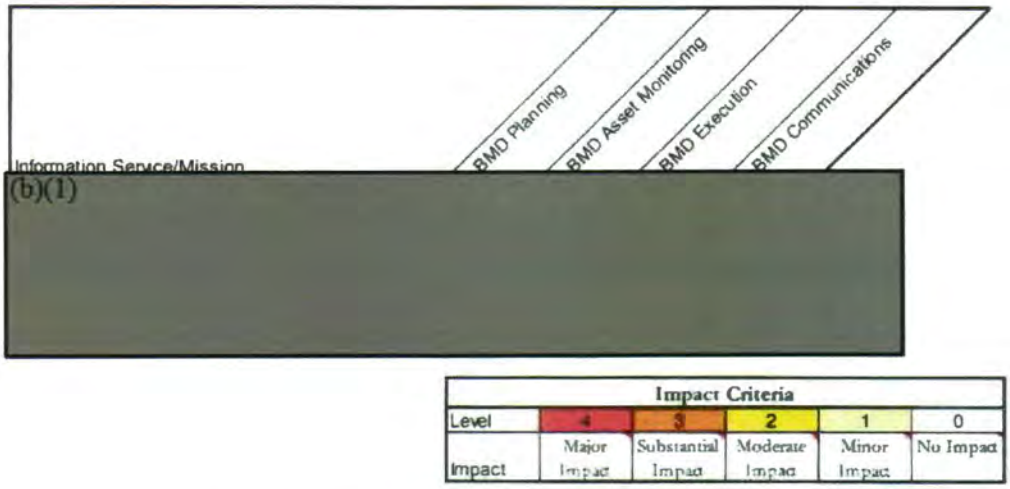
*Table 2 (U) C2BMC Information Services*

| Information Service | Description |
|---|---|
| C2BMC Planner | Builds, analyzes and develops the BMD plan that supports the Area Air Defense Commander (AADC) and the defended asset list (DAL). |
| Global Engagement Manager | Coordinates battle management engagement by managing sensor resources; multiple radars; situational awareness displays and data; and disseminates BMDS tracks. |
| Sensor Resource Management | Provides automated sensor resource tasking and monitoring. (b)(1) |
| Situational Awareness Data Feeds | Delivers information layouts via maps, displays, tracks, and alert messages through CCMD web browser, (b)(1) |
| BMDS Track Management | Implements capabilities to correlate early warning data from multiple sources. |
| BMDS Track Dissemination | Receive and forward system tracks, Link 16 tracks and GMD tracks |
| C2BMC Services | Manages engagement timelines, CCMD essential elements of information (EEI) and IBMP information through the collection and representation of links (b)(1) and nodes, information assurance, and database management services |

*Table 3 (U) C2BMC Data Sets*

| Data Sets | Description |
|---|---|
| BMD Track Data | Track information about BMD threats |
| Sensor Tasking | Information on sensor tasking for early warning and track coverage |
| Engagement Status Data | Information on status of engagement forces including capability and capacity for engaging threats |
| Sensor Status | Health and status information on the various sensor platforms |

(U) With the list of information services and data sets provided by C2BMC to support missions, a determination must be made of mission or task impact should a service be unavailable or the security of a data set be compromised. This provides the dependency model and half of the impact assessment for the risk analysis. For the information service availability impact, **Error! Reference source not found.** below illustrates the impact on each mission given a complete loss of availability for the services listed above. The assessment criteria for assigning impact levels are available in the NRAT Analyst Manual.




| Impact Criteria | | | | | |
|---|---|---|---|---|---|
| Level | 4 | 3 | 2 | 1 | 0 |
| Impact | Major Impact | Substantial Impact | Moderate Impact | Minor Impact | No Impact |

*Figure 2 [redacted] Mission Impact from Service Unavailability*

(U) Data security impact is performed with respect to loss of confidentiality and loss of integrity of each data source. Figure 3 illustrates the mission impact from compromise of data confidentiality from the various data sets. Figure 4 shows the mission impact from loss of data integrity from each of the data sets.

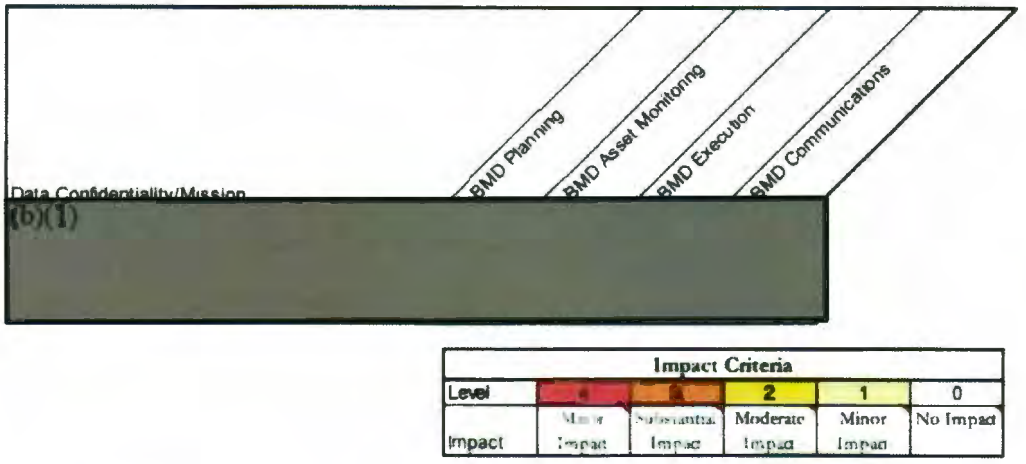



*Figure 3 [redacted] Mission Impact from Loss of Data Confidentiality*

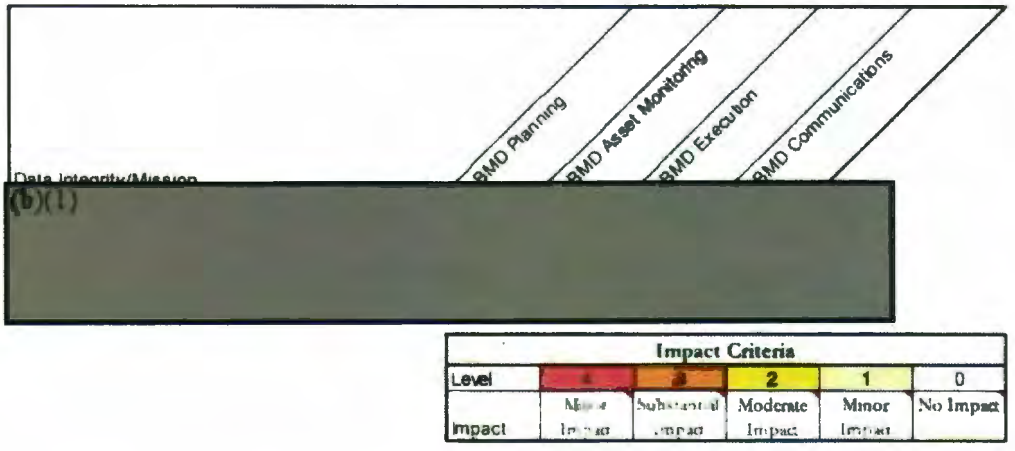



*Figure [redacted] Mission Impact from Loss of Data Integrity*

## 6 (U) Threat Actions

(U) What drives risk is the potential for the information services and data security to be compromised is intentional or unintentional actions against C2BMC. For the purposes of this analysis we consider cyber threat actions (also known as cyber attacks and exploitation) that are plausible and have the potential to compromise confidentiality, integrity, and or availability of C2BMC data and services. These actions are not associated with any particular cyber aggressor; however, in the general sense, the threat actions used in this preliminary analysis represent a range of sophistication and intended effects.

(b)(1)

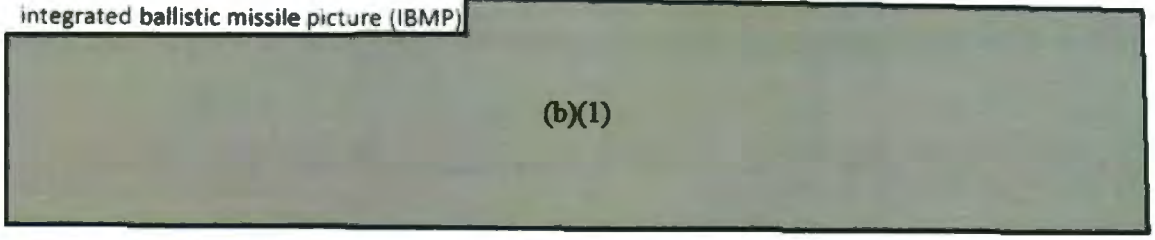
[redacted]

(b)(1)

## 5.1 (U) Data Compromise

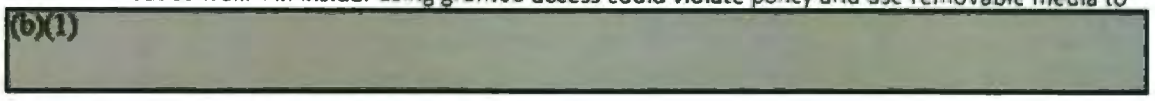
(S/[redacted]) C2BMC message processing data, ballistic missile track reports, engagement status, and the integrated ballistic missile picture (IBMP)

(b)(1)



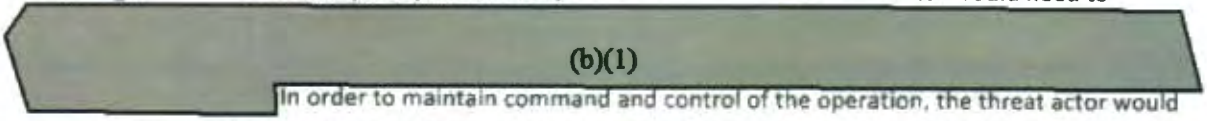
(S/[redacted]) Not only can data compromise come from an external attacker, compromise can come from an insider threat as well. An insider using granted access could violate policy and use removable media to

(b)(1)



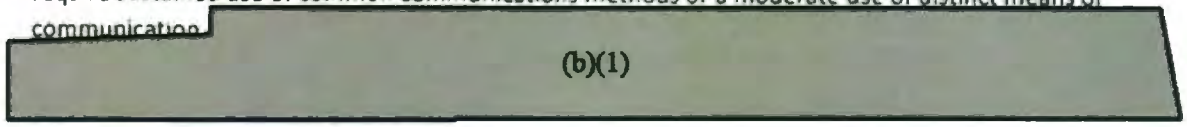
(S/[redacted]) In order to effectively compromise data, an external or internal threat actor would need to

(b)(1)



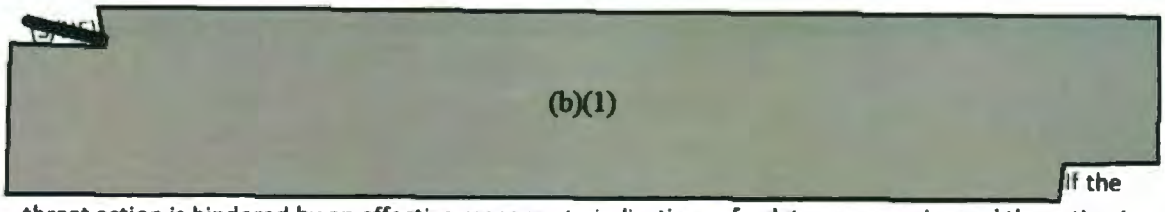
In order to maintain command and control of the operation, the threat actor would require sustained use of common communications methods or a moderate use of distinct means of communication.

(b)(1)



(S/[redacted])

(b)(1)



If the threat action is hindered by an effective response to indications of a data compromise and the action is



[redacted]

terminated, some reactionary steps could be taken to considerably lessen the impact of the compromise on BMD operations.

### 6.2 (U) Data Manipulation

(S/NF) External and internal attacks can also breach C2BMC data integrity by arbitrarily or deliberately manipulating data.

(b)(1)

(S/NF) A stealthier, more pernicious threat actor might deliberately manipulate C2BMC

(b)(1)

(S/NF) In general, a threat actor conducting arbitrary or deliberate data manipulation would be

(b)(1)

Once the system's architecture, services and data constructs are understood, a threat actor conducting arbitrary manipulation

Arbitrary manipulation might require

But, a deliberate manipulation might

(b)(1)

An arbitrary attack would require

A deliberate attack would likely require the

(b)(1) If C2BMC operators or administrators detect data manipulation, there

(b)(1)

(S/NF) The level of (b)(1)

(b)(1) Or for deliberate data manipulation, the (b)(1)

(b)(1)

(b)(1)

(b)(1) In order to effectively manipulate data, the threat actor will have (b)(1)

(b)(1) Once arbitrary data manipulation begins, (b)(1)

(b)(1) network operators and administrators. On the other hand, deliberate data manipulation (b)(1) (b)(1) In order to be effective, arbitrary and deliberate data manipulation (b)(1) (b)(1) (b)(1) (b)(1)

### 6.3 (U) Denial of Service (DoS)

(S//NF) External and internal attackers can also impact information availability by conducting denial of service (DoS) attacks on the CNIP. (b)(1) (b)(1) (b)(1) (b)(1)

(S//NF) A threat actor conducting a DoS attack against the (b)(1) (b)(1) (b)(1) Once the DoS is initiated, the threat actor (b)(1) (b)(1) attack. (b)(1) (b)(1) the threat actor (b)(1)

(S//NF) The threat actor would employ DoS technologies which have some elements of originality and could be tailored for the C2BMC environment. A security-aware operator or administrator would likely (b)(1) (b)(1) reactionary steps could be taken to considerably lessen the impact on C2BMC operations.

[redacted]

### 6.4 (U) Threat Actions Assessment

(U) The following threat actions were derived from review of existing C2BMC documentation and previous threat analysis, risk assessment, and exercise reports. The list is not intended to be exhaustive but rather a sampling of the potential cyber threats against C2BMC that span a range of likelihoods and potential impacts which is intended to inform a more detailed analysis into specific threats to represent in live evaluations of the architecture, protection, and response. The threat actions are assessed below according to NRAT methodologies as applied to preliminary understanding of C2BMC architecture; databases and services; and an attacker's objective to breach C2BMC information confidentiality, integrity or availability.

*Table 4 [redacted] Threat Action List*

| Ref | Description |
|---|---|
| 1A | (b)(1) (b)(1) While not specifically targeting specific information, looks to obtain as much information as possible in a short amount of time. Duration of presence is not as valuable as the amount of immediate data obtained. |
| 1B | (b)(1) Adversary targets specific information, looking to observe system behavior and monitor for data flow and use. Duration of presence is prioritized above that of exfiltrated data. |
| 1C | Insider Data Exfiltration – Insider uses granted accesses but knowingly violates removable media polity (b)(1) (b)(1) Data is burned to removable media and taken outside the secure perimeter for transmittal to adversary. |
| 2A | (b)(1) |
| 2B | |
| 2C | |



[redacted]

[redacted]

| Ref | Description |
|---|---|
| 3A | Insider introduction of malicious software – Insider introduces malicious logic through use of removable media during routine data transfer procedures. After a period of time, the malicious code activates and begins reconnaissance of local network looking for additional vulnerabilities. After a period of time, the malicious software begins a denial of service attack by disabling network interface cards and changing passwords. |
| 3B | (b)(1) |

[redacted] The first assessment below is the impact each threat action would have on the service availability, data confidentiality, or data integrity given the action successfully achieves the actor's objective. In this case, the assignment of impact was performed using the impact criteria listed in the NRAT Analyst Manual. Figure 5 shows the impact of each action on service availability. Figure 6 shows the impact on data confidentiality. Figure 7 presents the impact of each action on data integrity.



[redacted]

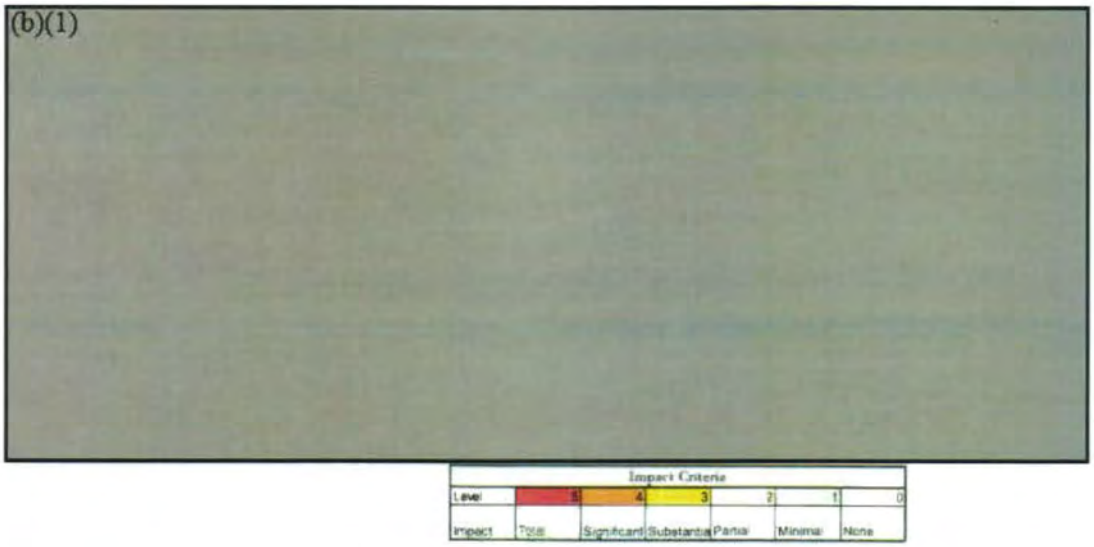



*Figure 5 [redacted] Threat Action Impact on Service Availability*

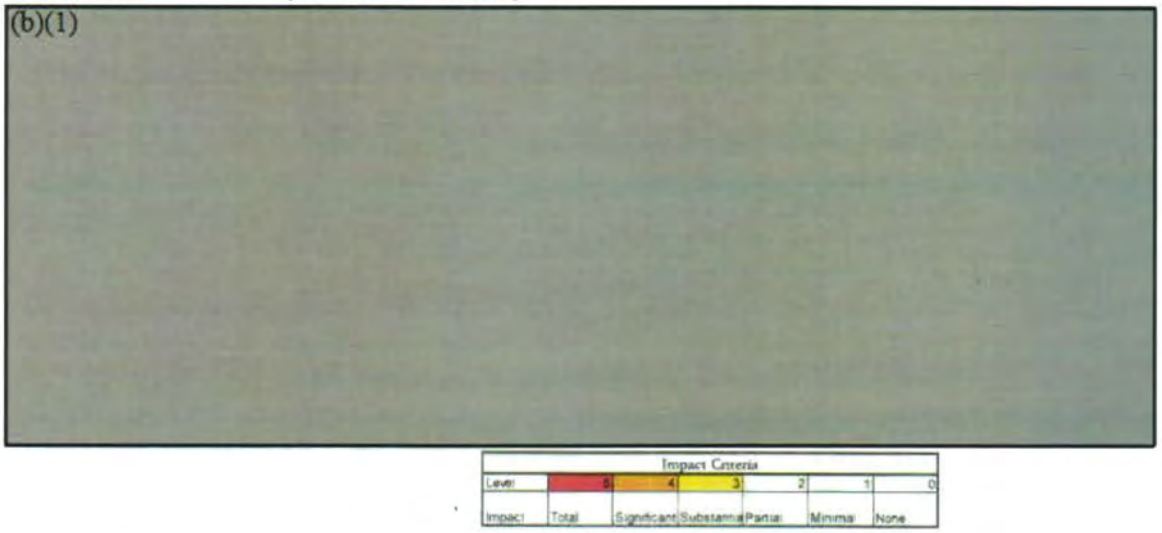



*Figure 6 [redacted] Threat Action Impact on Data Confidentiality*

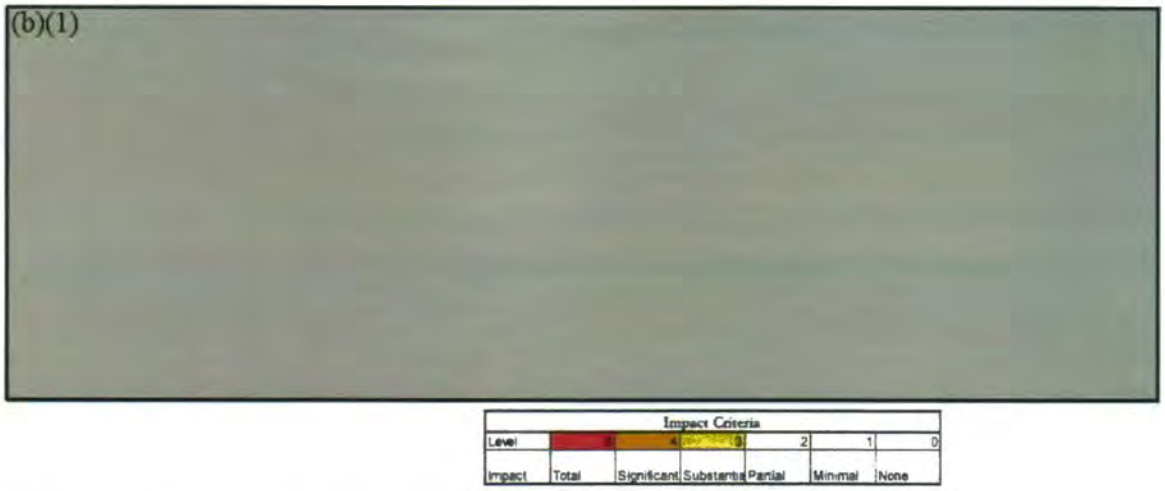



*Figure 7 [redacted] Threat Action Impact on Data Integrity*

[redacted] The next assessment that occurs is that with respect to characteristics of each threat action that make it more or less attractive for a threat actor to be capable and willing to carry out as well as those traits of a threat action that make it easier or harder to protect, detect, and respond against. The NRAT methodology specifies a set of questions to characterize these attributes. Appendix C lists the questions available from the NRAT Analyst manual and assessment made for the threat actions in Table 4 and Figure 8 below shows the attribute characterization from the NRAT methodology.

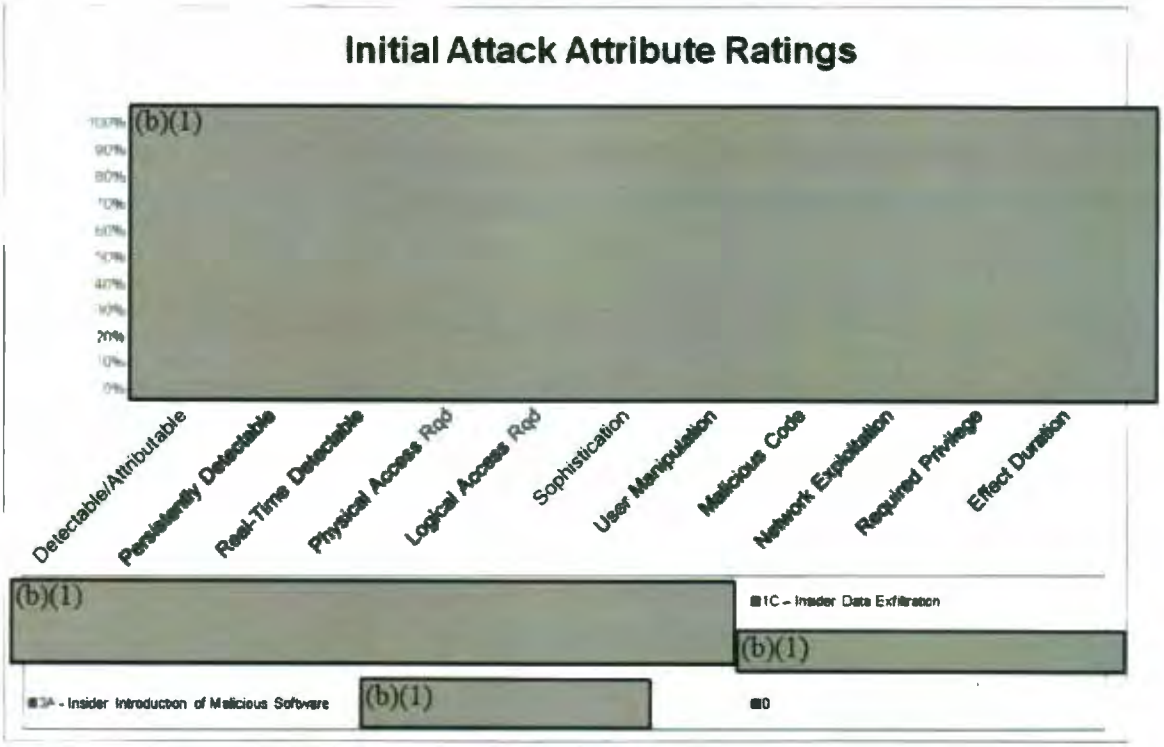



*Figure [redacted] Threat Action Characterization*

# 7 (U) Threat Actors[1]

## 7.1 (U) Nation-state

(S//[redacted] According to NASIC, (b)(1) (b)(1) Although (b)(1) (b)(1) conduct a cyber attack the BMDS (b)(1) However, (b)(1) exploiting DoD networks to obtain sensitive-but classified (SBU) information on U.S. technologies, including BMDS capabilities and data sources. (b)(1) BMDS and its C2BMC components.

## 7.2 (U) Rogue

(S//[redacted] Rogue threat actors include trusted insiders, external actors, social engineering actors, and supply chain counterfeiters with malicious intent. Trusted insiders might be disgruntled military, civilian or contracted staff with working knowledge and access to the C2BMC. External actors include hackers, script kiddies, cyber criminal groups, or terrorists who might deploy viruses, conduct DoS attacks, or

[1] (S//[redacted] July 2011, USSTRATCOM and MDA. Joint Report to Congress: Missile Defense Network Protection

[redacted]

espionage. Social engineering actors will use phishing techniques in order to gain access and escalate privileges in order to attack the C2BMC system. Lastly, supply chain counterfeiters could develop information technology (IT) components and software code that can be inserted surreptitiously into the supply chain and ultimately disrupt the C2BMC system.

### 7.3 (U) Unintentional

(S//REL) The C2BMC system might also be affected by unintentional threat actors like commercial software developers who implement faulty software into components that allows opportunities for hackers to penetrate the network. Or, trusted users who are insufficiently trained, employ weak passwords, inadvertently corrupt data, or mistakenly download malicious code.

(S//REL) For the purposes of this preliminary assessment, [redacted] from a previous [redacted] (b)(1) [redacted] For an updated assessment, the intelligence community should be sought to identify the list of

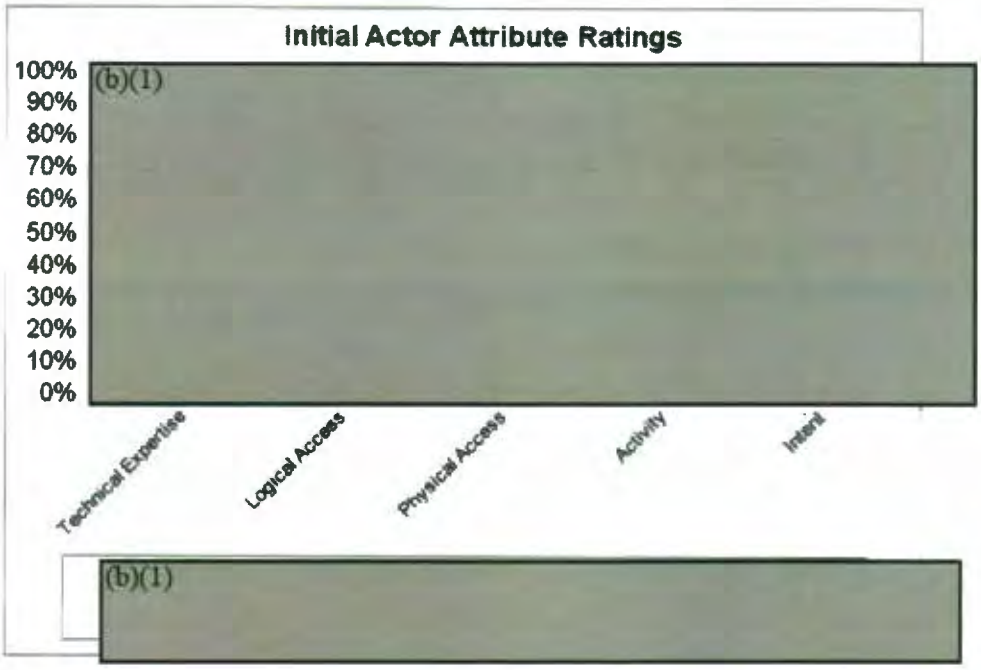



*Figure 9 (S//REL) Preliminary Threat Actor Attribute Ratings*

## 8 (U) C2BMC System Protections

(S//REL) The BMDS implements a robust defense-in-depth IA architecture that provides cybersecurity to the C2BMC system and protection against cyber incidents and CNA. The BMDS Network Operations and Security Center (BNOSC) enhances Tier 3 CNDSP functions which include all



[redacted]

C2BMC locations. These functions include network protection; monitoring; analysis and detection; and response.

(U//FOUO) However, C2BMC system protections begin with the acquisitions process. Hardware and software vulnerabilities, which can be introduced within the commercial-off-the-shelf acquisition process, are mitigated through a procurement review by the MDA's counter-intelligence organization. This organization ensures that hardware and software are thoroughly evaluated and procurement originates from trusted vendors. The MDA also reviews the BMDS IA architecture before component fielding to ensure standards for configuration and trustworthiness are met. Additionally, the agency conducts soak tests on BMDS architecture including C2BMC in order to stress activity loads on hardware and software. Lastly, USSTRATCOM and MDA manage a robust IA Vulnerability Management (IAVM) program that ensures software patching, upgrades and replacements are implemented.

(b)(1)

(U//FOUO) Distributed network architecture and interface vulnerabilities are mitigated (b)(1) And because BMDS sites provide diversity of path and media, C2BMC information and data can be transmitted and received (b)(1) (b)(1) These structures provide additional resilience in C2BMC information availability.

(U//FOUO) C2BMC system services rely on the CNDSP structure to provide around-the-clock monitoring, detection and response to network probes and attacks. Watch officers on the network are alerted to potential cyber attacks by special monitoring and alert management applications provided by the Defense Information Systems Agency (DISA) CONUS Operational Support Center (OSC).

(U) Infrastructure vulnerabilities within the Secret Internet Protocol Router Network (SIPRNET) and Non-classified Internet Protocol Router Network (NIPRNET) are mitigated by (b)(1) (b)(1) Defense Industrial Base (DIB). Additionally, the MDA established (b)(1) (b)(1) (b)(1) which support BMDS exercises, wargames, and tests. (b)(1) (b)(1) (b)(1) This process requires that the MDA Designated Accrediting Authority (DAA) must concur with all established procedures, terms and conditions which drive security and risk management.

(U) Lastly, the C2BMC has been subjected to multiple cyber vulnerability analyses from the Defense Intelligence Agency (DIA), National Air and Space Intelligence Center (NASIC), the Air Force Office of

Special Investigations (AFOSI), the National Security Agency (NSA), and DISA over the last decade. These assessments determined that C2BMC (b)(1) In addition to these cyber vulnerability assessments, MDA

(U//FOUO) The NRAT methodology uses a survey of 82 questions to assess the protection posture of the network with respect to protecting, defending, and responding to threat activities. The assessment of the protection posture was made by the authors referencing the information cited in the preceding paragraphs and utilizing assessments made of SIPRNET enclaves from previous studies. This provides a baseline assessment but it needs to be updated with responses of SMEs familiar with the protection mechanisms in place for the deployed C2BMC system. The assessment is presented only to provide the characterization needed to compute the preliminary risk results in the following section. Figure 1 below shows the protection ratings based on the preliminary assessment from available information.


*Figure 10 (U) Preliminary C2BMC Protection Posture*

## 9 (U) C2BMC Risk Analysis

(U) As discussed previously, the analysis performed in this report is based upon assessments of the various risk elements by the authors through research of available documentation. The assessments should be updated with SMEs of the system, threats, and operators. The risk analysis also is bounded by

(S//REL) July 2011, USSTRATCOM and MDA. Joint Report to Congress: Missile Defense Network Protection

[redacted]

the C2BMC system itself and does not extend to include all of the BMD system-of-systems. For example, a threat action may have a completely detrimental effect on a C2BMC suite but the overall BMD system of systems has the ability to shift responsibilities to another C2BMC suite given the loss of the single or primary suite. The analysis also does not include higher-level missions supporting a CCMD at this time. It may be useful to extend the analysis in the future to address those other dependencies to inform other processes and concept of operations (CONOPs).

### 9.1 (U) Threat Action – Mission Impact

(U) Using the NRAT risk methodology, risk is a product of the impact of successful threat actions and the likelihood an actor will successfully employ the threat action against the system. From Figure 1 above, the impact of a successful threat action is computed by combining the impact from threat actions on information services with the impact of information service loss on missions. Using the impact computation methodology from the NRAT Analyst Manual, Figure 11 illustrates the impact level of successful accomplishment of each threat action.

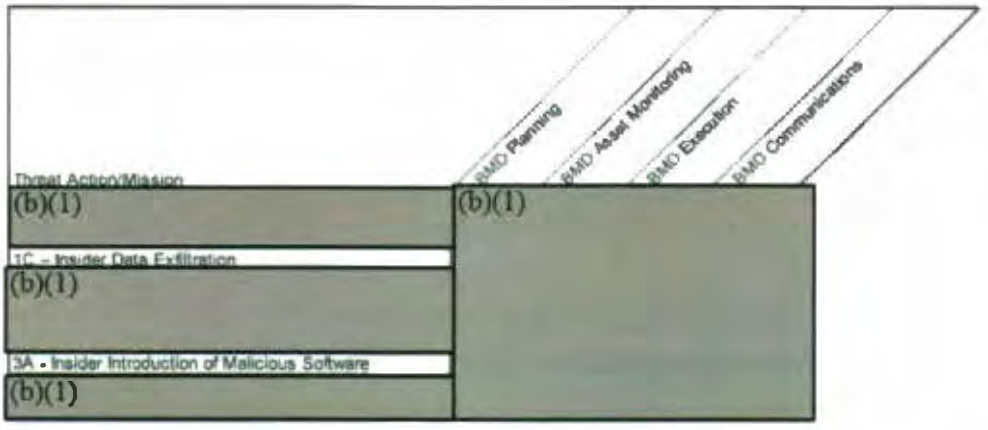



*Figure 11 [redacted] Mission Impact Given Successful Threat Action*

### 9.2 (U) Threat Action Likelihood

[redacted] From the NRAT Analyst Manual, threat action likelihood is the combination of threat actors' competency to carry out a threat action and the vulnerability of the system being targeted. Figure 12 displays the actor competency results for each threat actor and each threat action. Figure 13 shows the system vulnerability level of the current protection posture from each threat action. Finally Figure 14 illustrates the likelihood of each threat action given the most competent actor. In the case of the preliminary data used in this analysis, (b)(1) competent actor for each action.



[redacted]

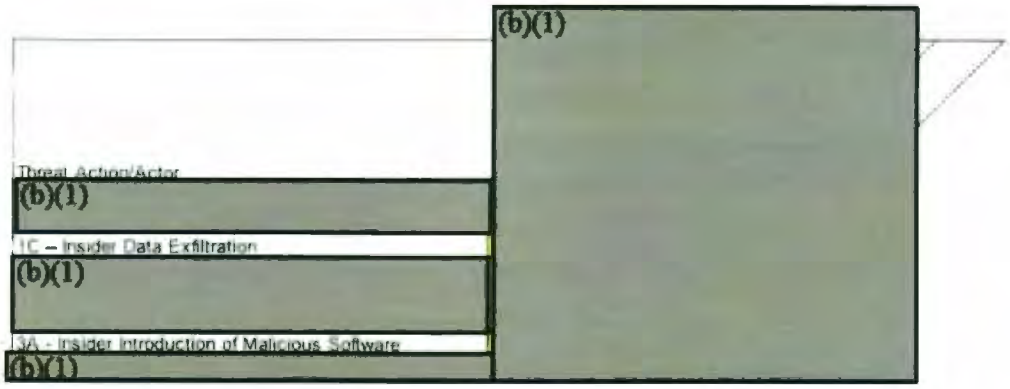



*Figure 12 [redacted] Actor Competency Results*

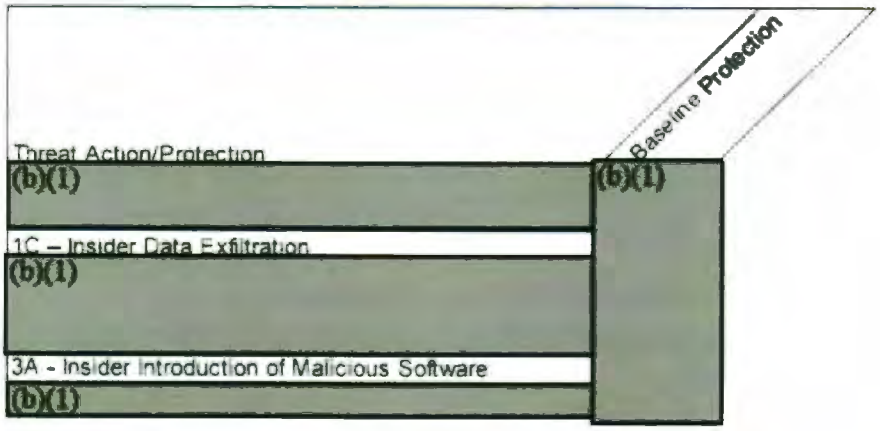



*Figure 1[redacted] System Vulnerability Results*

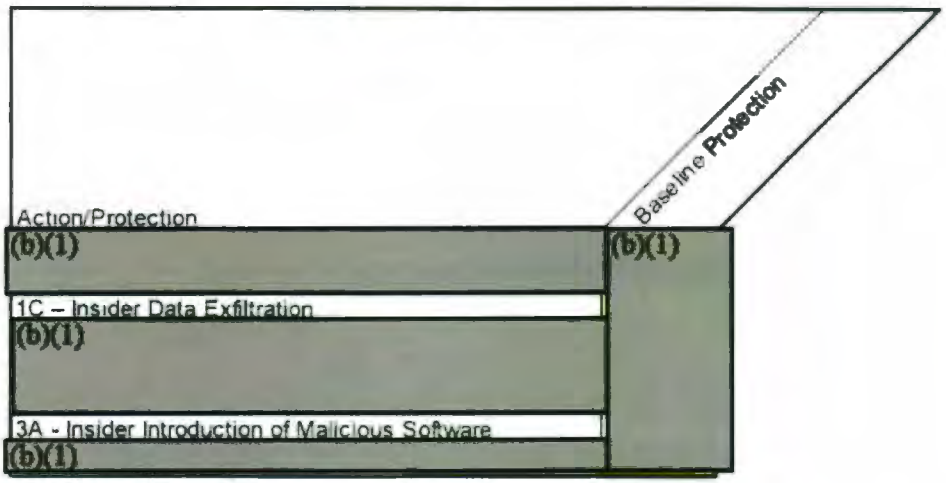



*Figure 14 (b)(1) Threat Action Likelihood Results*

### (U) Risk to C2BMC Missions

(U) To complete the risk assessment process, NRAT combines the likelihood and impact of a given threat action against the mission under evaluation. The following figures provide the mission risk for each threat action on BMD Planning (Figure 15), BMD Asset Awareness (Figure 16), BMD Execution (Figure 17), and BMD Communications (Figure 18). The cross-product of likelihood and impact provide the risk level indicated by the areas of risk going from low risk in the lower-left portions of the charts to high risk in the upper-right portions of the chart. From the preliminary analysis using the assessments and risk elements enumerated,

(b)(1)

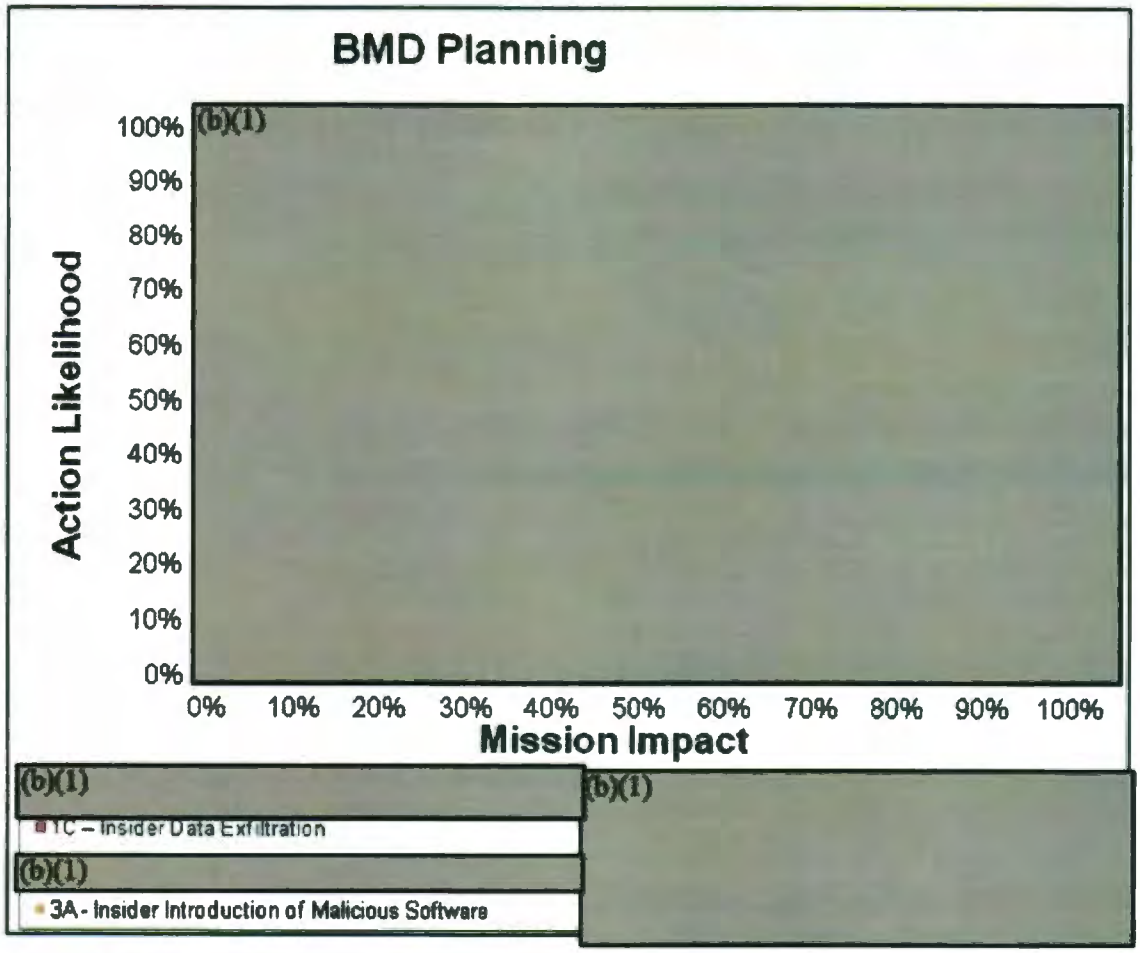



*Figure 15 [redacted] BMD Planning Risk*

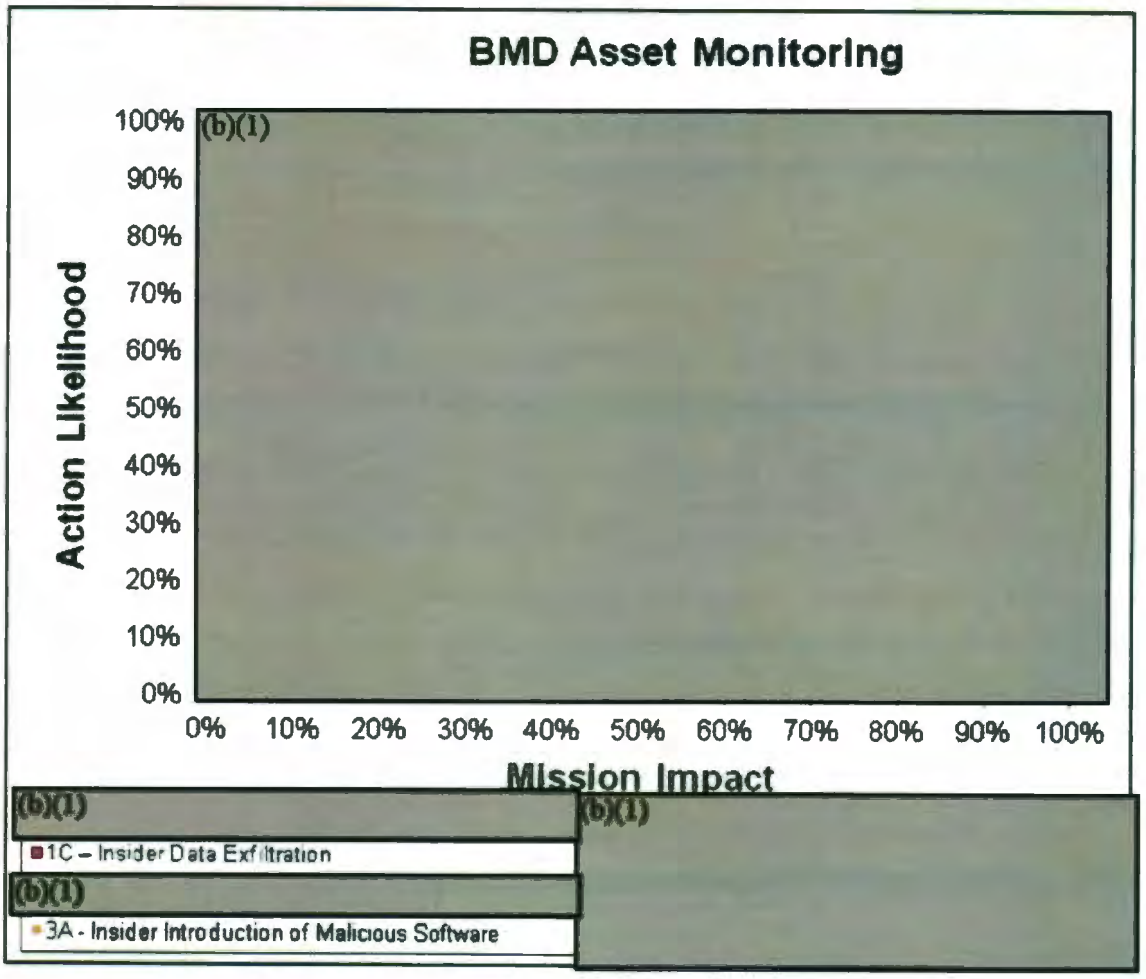



*Figure 16 [redacted] BMD Asset Monitoring Risk*

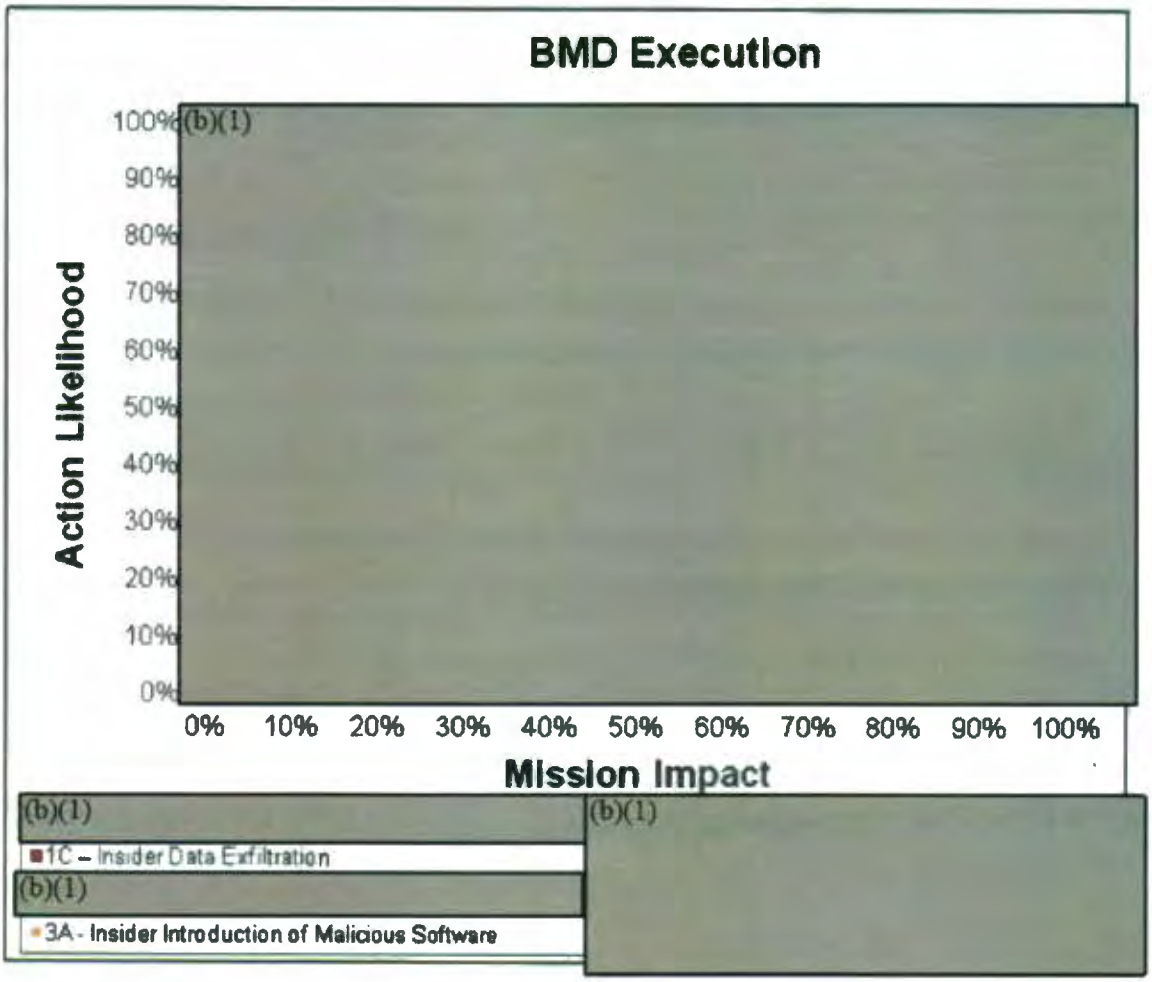



*Figure 1 [redacted] BMD Execution Risk*

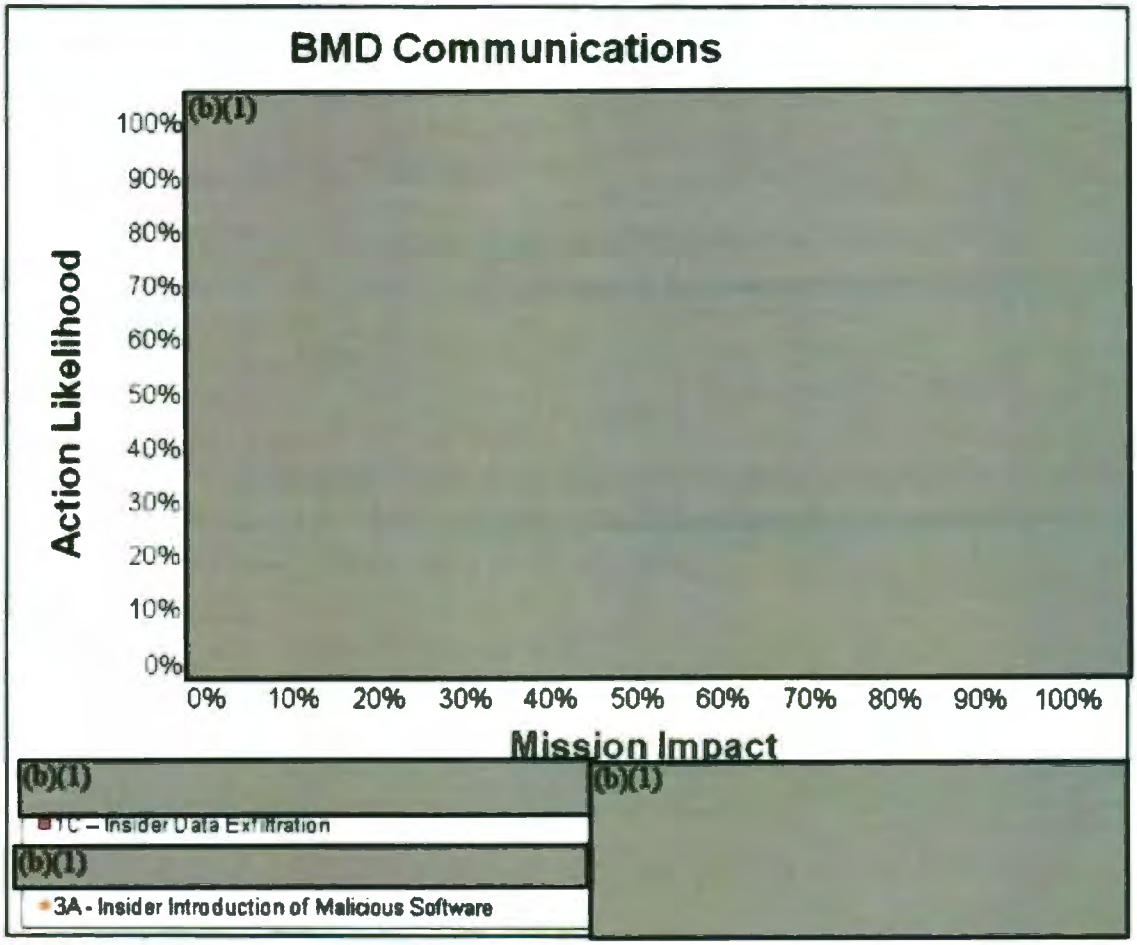



*Figure 1[redacted] BMD Communications Risk*

## 10 (U) Conclusion and Recommendation

[redacted] This preliminary cyber vulnerability assessment of the C2BMC system provides a foundation for more in-depth analysis of C2BMC cyber vulnerabilities using the NRAT capability alongside C2BMC experts. The employment of NRAT in future experiments or exercises involving C2BMC will likely yield more details about the degree of C2BMC cyber vulnerabilities relative to the system's operational employment. In other words, C2BMC vulnerabilities in the planning, monitoring and engagement phases of operations could be compared. Also, within each of these phases, an understanding of critical system dependencies and reactionary steps to data compromise, manipulation and DoS might be understood. Specifically, what reactionary steps currently exist within C2BMC employment practices and what mitigating effects do these have on threat actions? Are there system redundancies, data back-up protocols, or ambiguity resolution processes that would lessen the impact of cyber threat actions?

[redacted] Employing NRAT in the next C2BMC focused experiment or exercise would provide an opportunity to answer these questions and perhaps discover additional opportunities for C2BMC and BMD improvements. Therefore, it is recommended that cyber security analysts partner with BMD experts and begin coordinating efforts to deliver a C2BMC cyber vulnerability assessment with the full NRAT capability.

[redacted] It is recommended that, prior to using the results of this analysis, the inputs be reviewed by SMEs in each area of expertise required to make accurate and current assessments. SMEs in C2BMC architecture, security, operations, and intelligence communities who are familiar with credible threats to the system would be appropriate participants for future exercise or experiment opportunities. With an updated risk analysis, the results could be used to justify the need for additional vulnerability assessment and operational testing, or to narrow the scope of threat types to best represent operational impact. Detailed test plans could subsequently be developed to capture data from such events to provide confidence to Commanders in the ability of C2BMC to withstand cyber aggressors, inform acquisition programs for future capabilities, or to possibly aid in the development of TTPs for operation and response of the current system to fight through a contested cyber environment.

## (U) Appendix A – References

[redacted] January 2007, NASIC- "Computer Network Attack Threat to the US Ballistic Missile Defense System" [redacted]

[redacted] September 2007, Missile Defense Integration and Operation Center (MDIOC) GMD (b)(1) [redacted]

(U) September 2008, 92nd Information Operations Squadron (IOS) performed a scripted vulnerability assessment against the USNORTHCOM C2BMC infrastructure [redacted]

[redacted] September 2009, DIA Defense Intelligence Assessment – "Cyberthreat to Ballistic Missile Defense Programs" [redacted]

[redacted] (b)(1) [redacted]
(b)(1) [redacted]

[redacted] February 2010, Missile Defense Agency Cyber Intelligence Fusion Cell document, Computer Network Operations Collection Efforts Against MDA and the U.S. BMDS [redacted]

[redacted] May 2010, (b)(1) [redacted]
(b)(1) [redacted]

(U) September 2010, USSTRATCOM J86. Network Risk Assessment Tool (NRAT) Analyst's Manual for App Ver. 3.3 Revision 0 [redacted]

[redacted] USSTRATCOM JFCC IMD. "BMDS Cyber Assessment" IMD J6, LTC (b)(6) [redacted] in progress with a planned outbrief to CDRUSSTRATCOM 11 JAN 2011

[redacted] July 2011, USSTRATCOM and MDA. Joint Report to Congress: Missile Defense Network Protection

(U) October 2012, Missile Defense Agency (MDA). Ballistic Missile Defense System Handbook (U)

[redacted]

## (U) Appendix B - NRAT Assessment Attributes

### (U) Information System Protection Attributes

*(U) Real Time Monitoring* – The ability to monitor system activity in real time. Particularly, the ability to distinguish normal activity from threat action or pre-action activity. This includes consideration of intrusion detection or prevention systems as well as characteristics of the human components of system security.

*(U) Latent Monitoring* – The ability to post-process system activity and identify temporal performance trends or other subtle indicators of a "low and slow" threat action profile.

*(U) Physical Security* – The control of the physical space of information system components as well as communications to external systems, control of media and local port access, and dependencies upon external support systems. It also includes the potential for a compromised insider to provide physical access.

*(U) Virtual Boundary* – The logical access points into the information system. It includes perimeter systems such as demilitarized zones or demarcation zones (DMZ), simple boundary devices such as firewalls, as well as the policies and practices applied to routine communications through the boundary such as email and web services.

*(U) Privilege Regulation* – The methods by which authorized users are identified and authenticated to the system as well as the level of control and segregation of privileges among users and administrators.

*(U) User Awareness* – The degree to which users are aware of relevant threat profiles and to which users comply with sound security practices. This includes consideration of the effectiveness of education, monitoring, supervision, and policies.

*(U) Trusted Applications & Operating Systems* – The degree to which application and operating system software are controlled, screened, and trusted. This includes patch management and software configuration controls.

*(U) Hardened Network* – The ability to resist exploitation from an unauthorized source that has penetrated the virtual or physical boundary. This consideration is particularly oriented toward controls on network hardware.

*(U) System Recovery* – The ability to restore system operation following a compromise. This includes redundancies built into the system, the timeliness of system and data backups, and other potential means of consequence mitigation.

### (U) Threat Actor Attributes

*(U) Intent* – The desire of an actor to conduct cyber operations within the context of a particular target. This considers the level of tensions that may exist between the actor and the target, the actor's perception of obtaining a payoff, and the perceived likelihood and consequences of potential retribution.



[redacted]

*(U) Activity* – The degree to which the actor is active in the target's information domain. This includes experience with or knowledge of previous cyber attacks, cyber probes, and traditional intelligence collection activities or opportunities.

*(U) Logical Access* – The ability of the actor to exploit an information system to gain access and privilege.

*(U) Physical Access* – The ability of the actor to gain physical (contact or proximity) access to an information system either by exploiting authorized insiders or directly by other unauthorized means.

*(U) Technical Expertise* – The ability of the actor to possess or acquire the knowledge, skills, and resources to conduct threat actions. In general, greater technical expertise indicates an actor is capable of developing and executing more sophisticated threat actions.

### (U) Threat Action Attributes

*(U) Real Time Detectability* – The ability for the threat action to be detected as it occurs. That is, the degree to which the threat action is "noisy."

*(U) Persistent Detectability* – The ability for the threat action to be detected by latent means, such as system log reviews. This includes threat actions that are required to have precursor artifacts (i.e. configuration changes, system setting changes, etc.) on the target system for a period of time prior to actual execution of the threat action or to be present on the system for an extended period of time following execution in order to sustain an effect.

*(U) Physical Access* – The degree to which the threat action requires physical proximity to the target system or has elements that are physically detectable, such as electromagnetic emanations.

*(U) Logical Access* – The degree to which the threat action requires an opposed penetration of a logical perimeter into the target system.

*(U) User Manipulation* – The degree to which the threat action requires the unwitting participation (action or inaction) of authorized system users in order to be effective. This also considers the degree to which the threat action leverages masking, spoofing, or implied trusts to exploit the system's user(s).

*(U) Malicious Code* – The sophistication of the code or techniques used in the threat action. This includes consideration of the originality, complexity, and degree to which the code is specific to the target environment.

*(U) Network Exploitation* – The breadth and depth to which the threat action must traverse or otherwise influence the target system in order to be effective. This includes the number and nature of components that must be compromised.

*(U) Required Privilege* – The level of privilege that the threat action must attain in order to be introduced and executed.

[redacted]

*(U) Effect Duration* – The requirement for the threat action to sustain some effect over a period of time in order to be considered successful. The difficulty of this requirement may be mitigated by the degree to which the capability uses misdirection, masking, spoofing, or other means to confuse discovery, diagnosis, and recovery processes.



[redacted]

[redacted]

(U) Appendix I – Survey of CNE/CNA Attack Attributes and Threat Ratings

## 3. (U) THREAT ACTION RATING

### *3.1 (U) Detectable/Attributable*

#### 3.1.1 (U) Persistently Detectable

##### *3.1.1(1) (U) Pre-Initiation Persistence*

*(U) In some threat scenarios the actor has some presence on the target system prior to initiation of the attack, exploitation, or payload. This may include exploration of the network to identify vulnerable nodes, determining the location of desired data or components, pre-positioning a back door or other code to wait for the desired time of attack, or other preparatory activities. In some instances, these persistent activities may be detected after they occur through latent monitoring means such as log reviews and trend analysis such that the threat may be responded to and defeated before the actual execution.*

***(U) This question assesses the length of time (if any) that these preparatory activities or their artifacts are expected to be sustained on the target system prior to actual execution.***

| (U) How long is the actor expected or observed to have presence on the target system prior to initiation of the attack, exploitation, or payload? | | |
|---|---|---|
| Prolonged – 100 | Continuous for at least several months. | (b)(1) |
| Extensive – 80 | Intermittent over several months | |
| Moderate – 60 | Several weeks | |
| Limited – 40 | A week or less | |
| Short – 20 | Up to a few days | |
| None Required – 0 | No precursor presence expected | |

##### *3.1.1(2) (U) Post-Initiation Persistence*

*(U) In some threat scenarios the actor maintains some presence on the target system after initiation of the attack, exploitation, or payload. Reasons for sustained presence may include exfiltration of large volumes of data, monitoring system responses, and taking additional action to disrupt recovery or otherwise sustain an effect. In some instances, this sustained presence may enable detection after it occurs through latent monitoring means. As a result, a response may be mounted to prevent the actor's objectives from being fully realized and/or may mitigate impact to the targeted system.*



[redacted]

***(U) This question assesses the duration of threat presence after initiation of the attack, exploitation, or payload and prior to realization of the actor's full desired effect or target system impact.***

| (U) What is the duration of any expected or observed threat activity on the targeted system after initiation of the attack, exploitation or payload execution? | | |
|---|---|---|
| Prolonged – 100 | Continuous for at least several months. | (b)(1) |
| Extensive – 80 | Intermittent over several months | |
| Moderate – 60 | Several weeks | |
| Limited – 40 | A week or less | |
| Short – 20 | Up to a few days | |
| None Required – 0 | No presence expected after initiation of the attack or exploitation | |

### *3.1.1(3) (U) Concealment*

*(U) Some threat scenarios may have a presence on the target system prior to, during, and following execution, but that presence may be well concealed to evade detection by system logs, trend analysis, and other means of latent monitoring. Concealment activities may include log manipulation, kernel level or other "under the radar" operations, masquerading as legitimate system processes, use of polymorphic code, or encrypted or low profile communications.*

***(U) This question assesses the methods used by the threat to evade recognition of any persistent presence or artifacts as having malicious intent/origins.***

| (U) To what degree does the threat employ measures to avoid detection and characterization by latent monitoring means by changing its behavior, digital fingerprint, or other means (i.e. masking or spoofing effects)? | | |
|---|---|---|
| None – 100 | The operation is overt in nature and does not attempt to evade detection. Uses commands and techniques with known malicious intent. | (b)(1) |
| Some – 75 | The persistent presence is observable, but attempts to hide activity in common application behavior and communications. | |
| Moderate – 50 | The persistent presence is masked from association with common malicious activity profiles. | |
| Extensive – 25 | The persistent presence is superbly masked via log modification, connection hopping, polymorphic code, kernel level or other "under the radar" operations, or other state-of-the-art techniques. | |
| N/A – 0 | There are no activities detectable by latent monitoring means associated with the threat action. | |

[redacted]

### 3.1.2 (U) Real-Time Detectable

#### *3.1.2(1) (U) Pre-Initiation Activity Level*

*(U) In some threat scenarios the actor has some presence on the target system prior to initiation of the attack, exploitation, or payload. This may include footprinting, scanning, enumeration, and exploration of the network to identify vulnerable nodes or the location of desired data or components, pre-positioning a back door or other code to wait for the desired time of attack, or other preparatory activities. In some instances, these activities may be detected as they occur by real time system activity monitoring such as alerts from intrusion detection sensors or firewalls such that the threat may be responded to and mitigated before the actual execution.*

***(U) This question assesses the level of activity (if any) prior to execution or payload delivery to support command & control or other communications and/or malicious system actions.***

| (U) What is the frequency and intensity of malicious actions before initiation of the intended effect or payload execution? | | (b)(1) |
|---|---|---|
| Prominent – 100 | Operation requires frequent communication, several system actions, or installation of unique artifacts prior to execution | |
| Moderate – 67 | Operation requires sustained use of common communication methods or moderate use of distinct communication methods | |
| Slight – 33 | Operation requires infrequent or short term activity | |
| None – 0 | No preparatory activity is expected or observed prior to execution or activity is of very short duration or otherwise undetectable as it occurs | |



[redacted]

[redacted]

### *3.1.2(2) (U) Post-Initiation Activity Level*

*(U) In some threat scenarios the actor maintains some presence on the target system after initiation of the attack, exploitation, or payload. Reasons for sustained presence may include exfiltration of large volumes of data, monitoring system responses, and taking additional action to disrupt recovery or otherwise sustain an effect. In some instances, this sustained presence may enable detection as it occurs (or shortly thereafter) through real-time system monitoring. As a result, a response may be mounted that could prevent the actor's objectives from being fully realized and/or may mitigate impact to the targeted system.*

***(U) This question assesses the level of activities (if any) are after initiation via its command & control or other communications and/or visible system actions until realization of the actor's full desired effect or target system impact.***

| (U) What is the frequency and intensity of malicious activity expected or observed on the target system after initiation of the attack, exploitation or payload execution? | | (b)(1) |
|---|---|---|
| Prominent – 100 | Operation requires sustained frequent communications, overt system actions, or unique and easily detected artifacts following execution | |
| Moderate – 67 | Operation requires moderate levels of sustained communications or performs system actions following execution that are generally consistent with common network activity | |
| Slight – 33 | Operation requires infrequent communications or short duration artifacts | |
| None – 0 | No activity is expected or observed and no identifiable artifacts remain once the operation is initiated. | |



[redacted]

### *3.1.2(3) (U) Signature Evasion*

*(U) Some threat scenarios may have a presence on the target system prior to, during, and following execution, but that presence may be well-concealed by evading signature or anomaly based detection and other traditional means of real time system monitoring and defense. Examples may include use of polymorphic code, masking effects of actions as common system activity, and encrypted or low profile communications.*

***(U) This question assesses the methods used by the threat to evade recognition of their actions as having malicious intent/origins as they occur.***

| (U) To what degree does the threat employ measures to avoid detection by sensors and avoid characterization by intrusion detection systems by changing its behavior, digital fingerprint, or other means (i.e. masking or spoofing effects)? | | (b)(1) |
|---|---|---|
| None – 100 | The operation is overt in nature and does not attempt to evade detection. Uses commands and techniques with known malicious intent. | |
| Some – 75 | The operation attempts to hide activity in common application behavior and communications. | |
| Moderate – 50 | The signature or effect is masked from association with common malicious signature profiles. | |
| Extensive – 25 | The signature is masked via polymorphic code or other state-of-the-art techniques or use of encryption to hide communications traffic content. | |
| N/A – 0 | There are no activities detectable in real time associated with the threat action. | |

### 3.1.3 (U) Attributable

#### *3.1.3(1) (U) TTPs & Technology Employed*

*(U) In some instances threat actors may be inhibited from conducting malicious actions if they believe that the actions may be attributed to them Evidence of the origin of a threat action may be provided by the technology employed, the tactics, techniques, and procedures (TTP) employed, or other signature behaviors.*

***(U) This question assesses the potential for threat action attribution to the actor or true origin. If direct physical access by the actor is used to carry out the action, a high level of attribution should be considered based on availability of physical and/or visual evidence.***

| (U) To what level does the signature, behavior (tactics, techniques, or procedures), or technologies employed in the threat action make it susceptible to attribution to the true origin? | | |
|---|---|---|
| Very High – 100 | The operation bears unmistakable signatures that are unique to the actor's specific identity by unbiased legal assessment. | (b)(1) |
| High – 67 | The operation bears clear signatures that are specific to the actor's culture or geo-location. May have indication of specific identity, but may not provide legal proof. | |
| Moderate – 33 | The operation is characteristic of TTPs from forums available to select hacker/cracker communities. May provide circumstantial evidence traceable toward actor identity. | |
| Low – 0 | Methods are commonly found in general forums, demonstrations, or training courses broadly available to the general populace. | |

*3.2 (U) Access*

**3.2.1 (U) Physical Access**

**3.2.1(1) (U) Proximity Requirement**

(U) *In some threat scenarios the actor will have some physical presence at or near the target system in order to complete the operation. This may include observing target system operations, placing portable media into target system devices, operating target system equipment, or limited range communication with the target system.*

***(U) This question assesses the difficulty in gaining any physical proximity needed for conducting the threat operation. If the threat actor is an insider or an insider is a participant in the threat action, then the degree of authorized access should be considered to mitigate the difficulty in achieving physical access and lower valued criteria selected.***

| (U) What is the physical proximity needed to pre-position or execute the operation? | | (b)(1) |
|---|---|---|
| Physical in Secure Area – 100 | Requires unauthorized covert physical contact with equipment in secure target area. | |
| Physical in Unauthorized Area – 83 | Requires some physical interface with target system above authorization level. | |
| Physical in Non-Secure Area – 66 | Requires unauthorized physical contact with equipment in low-security target area. | |
| Perimeter near Secure Area – 49 | Requires unauthorized presence in a physical location within sight of secure target area. | |
| Perimeter near Non-Secure – 32 | Requires covert physical presence within sight of a low-security target area. | |
| Normal – 15 | Requires insider physical interface with target system at normal authorization. level | |
| None - 0 | No physical proximity is needed or expected for the operation. | |

[redacted]

### 3.2.1(2) (U) Physical Footprint

*(U) In some threat scenarios the actor will have some physical presence at or near the target system in order to complete the operation. This may include observing target system operations, placing portable media into target system devices, operating target system equipment, or limited range communication with the target system.*

***(U) This question assesses the difficulty in remaining undetected by visual or other physical means due to level of physical activity within proximity of the target environment. If the threat actor is an insider or an insider is a participant in the threat action, then the degree of authorized presence should be considered to mitigate the difficulty in achieving physical presence and lower valued criteria selected.***

| (U) What is the scope (footprint) of physical presence at or near the target environment? | | (b)(1) |
|---|---|---|
| Large and Distinct – 100 | Multi-person covert team with large/distinctive equipment. | |
| Large – 80 | Multi-person covert team with small/common equipment; OR<br><br>Insider in unauthorized area; OR Single-person with distinctive equipment. | |
| Moderate – 60 | Single person covert team with small/common equipment. | |
| Low – 40 | Insider with unauthorized media, portable equipment, in violation of policy. | |
| Very Low – 20 | Insider performing tasks with little potential for detection. | |
| None – 0 | No physical presence is needed or expected for the operation. | |



[redacted]

### 3.2.1(3) (U) Electromagnetic (EM) Footprint

*(U) In some threat scenarios the actor will have some physical presence at or near the target system in order to complete the operation. This may include observing target system operations, placing portable media into target system devices, operating target system equipment, or limited range communication with the target system.*

***(U) This question assesses the difficulty in remaining undetected by electromagnetic or other electronic means due to use of distinct electromagnetic (EM) signals in the target environment.***

| (U) What are the electromagnetic (EM) indicators of physical presence? | |
|---|---|
| Large and Overt – 100 | High power emanation of distinctive signal from within target area of control. |
| Large, but covert – 75 | High power emanation of distinctive signal within target area of influence but outside target's direct control. |
| Moderate – 50 | Low power emanation of distinctive signal OR High power emanation of common signal from within target area of control. |
| Low – 25 | Low power emanation of common signal within target area of control or influence. |
| None – 0 | No EM emanations. |

(b)(1)

### 3.2.2 (U) Logical Access

#### 3.2.2(1) (U) Identification of Entry Point

*(U) Many threat scenarios involve some level of logical access to the targeted system. The methods of achieving this access are numerous and diverse. To make an assessment of how difficult it will be to gain the access necessary to complete the threat scenario, NRAT considers two elements – (1) the identification or localization of a gateway or point of logical entry into the system, and (2) the penetration, circumvention, or other defeat of any security means or other inhibitors to gaining access through the gateway (if required)*

***(U) This question addresses the difficulty (time and/or expertise) of finding the entry point of the target information system. Searching and identification may include wardialing, wardriving, webcrawling, etc. If the threat action does not require locating a logical point of entry to a system, then "None" should be selected.***

| (U) How difficult will it be to locate the point of entry into the target network? | |
|---|---|
| Very Difficult – 100 | Entry point is intentionally concealed or disguised. Threat actor begins the operation with little or no foreknowledge of network connections. |
| Difficult – 75 | Requires exhaustive searching requiring extensive manual analysis. Susceptible to honeypots or other false indicators. |
| Moderate – 50 | Actor can use physical location or other foreknowledge to queue or filter the search. |
| Easy – 25 | Requires common scanning technique with common OS information prompting. |
| None – 0 | Entry point is already known or is not needed for the scenario. |

(b)(1)

### 3.2.2(2) (U) Boundary Access

*(U) Many threat scenarios involve some level of logical access to the targeted system. The methods of achieving this access are numerous and diverse. To make an assessment of how difficult it will be to gain the access necessary to complete the threat scenario, NRAT considers two elements – (1) the identification or localization of a gateway or point of logical entry into the system, and (2) the penetration, circumvention, or other defeat of any security means or other inhibitors to gaining access through the gateway (if required).*

***(U) This question assesses the difficulty of penetrating the boundary of the target system (this does not include interior mapping or privilege escalation). Criteria provide only example rating and to not accommodate all means or methods that may be applied. If the threat action does not require any penetration of protected boundaries, then "None" should be selected.***

| (U) What level of boundary restriction is the operation expected to penetrate in order to access the target network? | | (b)(1) |
|---|---|---|
| Very High – 100 | Complex perimeter protections such as a best practice DMZ configuration. | |
| High – 75 | Well configured perimeter router, firewall, and/or VPN Tunnel | |
| Moderate – 50 | Commonly configured perimeter router and/or firewall. | |
| Low – 25 | Minimally protected perimeter controls. | |
| None – 0 | No perimeter control device exists OR no penetration is needed OR insider with authorized access is used to gain entry to network | |

[redacted]

*3.3 (U) Complexity*

**3.3.1 (U) Sophistication**

**3.3.1(1) (U)** ***Degree of User Spoof (populated from 3.3.1.1(2))***

***3.3.1(2) (U) Technology Influence Mechanism***

*(U) The means by which a threat scenario exploits or manipulates the target system's information technology can be reflective of the technical sophistication needed by a threat actor to develop and employ the threat action. Some influence mechanisms, such as flooding a gateway or exploiting a documented application vulnerability call for relatively little ingenuity while developing new mechanisms that effect a broad range of environments or which cannot be easily patched against represent greater sophistication. This is distinct from the complexity of technology or tactics necessary to actually exploit the vulnerability which is covered separately.*

***(U) This question is intended to assess the degree of sophistication or ingenuity associated with the influence mechanism of the threat action. Some examples are provided in the criteria below, but in general simple/common methods should be assigned lower valued criteria while more original, intricate, or insidious mechanisms should be given higher values.***

| (U) How sophisticated is the threat action's means of technology influence? | | |
|---|---|---|
| Very high – 100 | The influence is highly intricate, original, and inherent to common information technology or is very precisely developed for a unique environment | (b)(1) |
| High – 75 | The influence mechanism has some elements of originality and would be difficult to remediate. Is broadly effective or is tailored for a specific environment. | |
| Moderate – 50 | The influence mechanism is derivative of known vulnerabilities | |
| Low – 25 | The influence mechanism is rudimentary in nature or is only effective in certain situations or conditions (e.g. unpatched software) | |
| None – 0 | | |



[redacted]

[redacted]

### *3.3.1.1 (U) User Manipulation*

#### *3.3.1.1(1) (U) User Participation*

*(U) Some threat actions employ social engineering techniques to lure unwitting system users into taking actions that unintentionally facilitate the threat scenario The attribute is characterized by the degree to which the action to be performed requires the user to violate best security practices and the degree to which the true nature of the actions are concealed. This consideration is distinct from compromising a user to intentionally perform malicious or supporting actions which is covered elsewhere in the model.*

***(U) This question is intended to assess the degree to which an unwitting target system user must act in a way to enable the attack or exploitation to succeed (click a link, open a file, provide password, etc.). If the user must perform actions that are in clear violation of sound practices, higher values should be selected or entered.***

| (U) What level of UNWITTING user participation is needed for the operation to succeed? | | |
|---|---|---|
| Very High – 100 | A user must blatantly violate common security practices. Example may include downloading, installing, and execution of a malicious application. | (b)(1) |
| High – 75 | A user must perform an action against best security practices. Example may include supplying authentication information over phone or email | |
| Moderate – 50 | A user must perform an action against good security practices or common actions without diligence or scrutiny. Example may include opening an email attachment or click on a link in an email. | |
| Low – 25 | A security-aware user may fall victim of the malicious action through a common action. Example may include opening an email appearing to be from a familiar source, visiting a popular or familiar website, or using a standard application to open file on trusted server. | |
| None – 0 | No unwitting user participation is needed. | |



[redacted]

### *3.3.1.1(2) (U) Degree of User Spoof*

*(U) Some threat actions employ social engineering techniques to lure unwitting system users into taking actions that unintentionally facilitate the threat scenario The attribute is characterized by the degree to which the action to be performed requires the user to violate best security practices and the degree to which the true nature of the actions are concealed. This consideration is distinct from compromising a user to intentionally perform malicious or supporting actions which is covered elsewhere in the model.*

***(U) This question is intended to assess the degree to which the unwitting system user is manipulated into performing some action that supports the attack or exploitation. Examples would be the use of spoofed trusted sites in links or email return addresses.***

| (U) What level of deception is used to elicit the participation of the user? | | (b)(1) |
|---|---|---|
| User Action without Spoof – 100 | User must take specific action with no spoofing attempted. | |
| Rudimentary Spoof – 83 | False labeling (of hyperlink, application extension). | |
| Social Engineering – 66 | Masquerading phone call (good social engineering content/interaction). | |
| Technical Replication – 49 | Use of similar names (knockoff website, different domain, spoofed email source). | |
| Spear Phishing – 32 | Phishing with full spoofing of site or email content. | |
| Website Corruption – 15 | Actual favorite or familiar website content corrupted. | |
| No User Involvement - 0 | No unwitting user participation is needed. | |

[redacted]

### *3.3.1.2 (U) Malicious Code and Tactics*

#### *3.3.1.2(1) (U) Complexity of Code & Tactics*

*(U) Some threat actions involve use of malicious code. Most will involve the development and employment of tactics, techniques, and procedures (TTP) in order to execute a sequence of actions that will result in some desired effect More complex code and TTPs are generally more difficult to protect against. For example, zero day code and innovative TTPs are less likely to be identified by automated means or be quickly recognized as malicious by system operators than threats with known profiles and fingerprints.*

***(U) This question is intended to assess the degree of sophistication an actor would require in order to develop the computer code and/or TTPs for the threat actions. More original and creative code (such as zero-day) or innovative tactic is assigned higher values and simple or existing code (such as downloadable exploits) is assigned lower values.***

| (U) What is the level of complexity and originality of the code or TTP used in the operation? | | (b)(1) |
|---|---|---|
| Original Zero Day – 100 | Completely original and complex code or TTP dissimilar to any known operation, exploiting un-known vulnerability. | |
| Expertly Modified – 80 | Expert modification of sophisticated code or TTP to exploit new vulnerability or effectively evade detection. | |
| Variant of familiar threat action – 60 | Modification of code or TTP from a previously known operation. May evade some signature-based detection schemes and alert users. | |
| Adapted Code – 40 | Superficially modified code or TTP of previous known operation. May evade simple signature-based detection schemes. | |
| Packaged Code – 20 | Directly downloaded code or duplicate TTP from previous known operation. | |
| N/A – 0 | No malicious code or original TTP employed. | |



[redacted]

[redacted]

*3.3.1.3 (U) Network Exploitation*

**3.3.1.3(1) (U) Depth of Traversal**

*(U) Once the threat is inside the virtual boundaries of the network, the threat scenario may necessitate traversing across the network to many nodes (breadth), penetrating deeper into the network to protected segments or enclaves (depth), and establishing system privileges to perform actions and/or compromise data.*

***(U) This question is intended to address the degree to which the threat scenario must identify and access or exploit selective components or data within the network in order to perform its activity. This process may include access to specific nodes, files, or data elements.***

| (U) What is the degree to which the target network has to be penetrated following entry (depth)? | | |
|---|---|---|
| Protected Segment – 100 | Must access an enclave or specific components within the target network which are very highly protected. This may include a network at a higher classification level or otherwise separated from the entry point by highly customized or monitored electronic guards or physical means. | (b)(1) |
| System Files – 75 | Must penetrate to system files or servers from low level entry point. | |
| Specific Files – 50 | Must locate specific files or data points on common network storage. | |
| General Network – 25 | General access to network data is sufficient. | |
| Entry Point – 0 | The network entry point is the only network point of interest. | |



[redacted]

### 3.3.1.3(2) (U) Breadth of Traversal

*(U) Once the threat is inside the virtual boundaries of the network, the threat scenario may necessitate traversing across the network to many nodes (breadth), penetrating deeper into the network to protected segments or enclaves (depth), and establishing system privileges to perform actions and/or compromise data to achieve the end goal of the threat actor*

***(U) This question is intended to address the degree to which the method must perpetuate across the network in order to perform its activity as needed to complete the actor's full intended end state. This process may include network mapping and compromise or circumnavigation of interior network partitions.***

| (U) What is the degree to which the target network nodes have to be accessed and/or exploited following entry (breadth)? | | |
|---|---|---|
| Entire Network – 100 | The capability must traverse across entire network and compromise majority of hosts and/or network devices. | (b)(1) |
| Multiple Hosts – 67 | The capability must traverse across several network segments and multiple hosts. | |
| Single Host – 33 | A single host within the network enclave is all that's needed for operation success. | |
| Entry Point – 0 | The entry point is the only network point of interest. | |

3.3.2 (U) System Privilege

**3.3.2(1) (U) Level of Privilege**

*(U) Once the threat is inside the virtual boundaries of the network, the threat scenario may necessitate traversing across the network to many nodes (breadth), penetrating deeper into the network to protected segments or enclaves (depth), and establishing system privileges to perform actions and/or compromise data to achieve the end goal of the threat actor.*

***(U) This question is intended to assess the level of difficulty for gaining adequate system privileges needed to complete the actor's full intended end state. The criteria below reflect a threat in a common client/server architecture. Other architectures or threat scenarios can be evaluated with the relative difficulty of obtaining needed permissions or privilege.***

| (U) What level of system privilege does the threat need to have in order to achieve the actor's end state objective? | | |
|---|---|---|
| Domain Admin – 100 | Access to highly protected databases, enclaves, or network device settings. | (b)(1) |
| Host Root – 80 | Full administrative or root level access. | |
| Power User – 60 | Super user access (application installation, web server upload, etc.). | |
| User – 40 | User level privilege. | |
| Guest – 20 | Guest level access. | |
| None – 0 | No privilege is needed. | |

***3.3.2(2) (U) Breadth of Traversal (populated from 3.3.1.3(2))***

3.4 (U) *Effect Intensity*

**3.4(1) (U) Prominence of Effect**

*(U) This is one of three questions that characterize the intensity of the effect of the threat action.*

***(U) This question is intended to assess the difficulty of sustaining the desired effect by drawing attention of system users, operators, and administrators. The more the effects are noticed and the degree to which they are recognized as having a malicious origin and intent, the swifter and concerted a response is expected. This question sets the degree to which the desired effect will disrupt information services and operations of the target system or otherwise elicit the attention of IT/security staff. For example, actions that exhibit a high degree of the intended effect would be rated "Extensive" or "Total", while actions that exhibit a very low degree of the intended effect may rate "Minor" or even "None"***

| (U) What is the degree to which the desired effect will disrupt the information services and operations of the target system or otherwise elicit the attention of network operators, administrators, and security staff? | | (b)(1) |
|---|---|---|
| Total – 100 | The operation disables or significantly inhibits all information services and commands immediate attention. Effects are clearly recognizable as having malicious origin and intent. | |
| Extensive – 75 | The operation disables or inhibits many normal services or at least one very critical service that would be immediately noticed. | |
| Noticeable – 50 | The operation disables or inhibits one or more information services that would be noticed by at least some users. –OR– The effect is evident, but the malicious origin/intent is masked or otherwise unclear. | |
| Minor – 25 | The effects could go unnoticed or unrecognized as having malicious origin/intent for a prolonged period of time depending on system conditions at the time of execution. | |
| None – 0 | The operation effect is unlikely to be noticed by system users or administrators. | |

[redacted]

**3.4(2) (U) Sustained Effect**

*(U) This is one of three questions that characterize the intensity of the effect of the threat action.*

***(U) This question is intended to assess the difficulty of sustaining the actor's desired effect as long as needed to achieve some desired condition or outcome. If it is otherwise known that system operations cannot be restored within the window of effect duration, then the selected value should be correspondingly reduced. Additionally, the selected value should be reduced to the degree that effective measures are employed to delay response to the action. This question sets the degree to which the threat actor needs the effect to be sustained in order to achieve the desired outcome. For example, effects that need to be sustained for more than 24 hours would be rated "Prolonged", while effects that require short amount of time may be rated "Several Minutes" or "Few Minutes".***

| (U) To what degree does the actor need for the effect to be sustained in order to achieve the desired condition or outcome? | | (b)(1) |
|---|---|---|
| Prolonged – 100 | The effects are desired to be sustained for more than one day with no substantial misdirection, distraction, or disruption employed to delay response actions. | |
| Several Hours – 80 | The effects are desired be sustained for several hours. –OR– The effect is desired to be sustained for more than a day, but has some measures to delay response. | |
| An hour or two – 60 | The effects must be sustained for more than an hour. –OR– The effect is desired to be sustained for longer, but has some measures to delay response. | |
| Several Minutes – 40 | The effects must be sustained for several minutes (around 30 minutes). –OR– The effect is desired to be sustained for longer, but has extensive measures to delay response. | |
| Few Minutes – 20 | The effects are only required to be sustained for a few minutes (less than 15). –OR– The effect is desired to be sustained for longer, but has extensive measures to delay response. | |
| Instantaneous – 0 | The desired effects are realized immediately. –OR– Effects cannot possibly be stopped once initiated. | |



[redacted]

[redacted]

**3.4(3) (U) Ability to Recover or Mitigate**

*(U) This is one of three questions that characterize the intensity of the effect of the threat action.*

***(U) This question is intended to assess the degree to which the threat actor's desired end state or outcome could be hindered by an effective response to indications of the action. Effective response, mitigation and recovery actions by the system operators and security staff could reduce the overall impact to the system from the threat action or accelerate system recovery. The extent to which the threat action integrates distraction, disruption, spoofing, or masking to delay responsive actions should be considered by selecting lower valued criteria. For example, if the threat action could be substantially mitigated by attentive IT staff, "Substantial" should be selected, if there is little that could be done by way of mitigation actions, "Minimal" should be selected.***

| (U) To what degree could the actor's desired end state or outcome be hindered by an effective response to indications of the action? | | (b)(1) |
|---|---|---|
| Full – 100 | An attentive network staff could substantially mitigate effects or promptly recover system operation such that minimal system degradation would occur. | |
| Substantial – 75 | Steps to mitigate the effects or quickly recover system operations could be taken such that the actor's desired conditions may not be fully realized. | |
| Partial – 50 | Some reactionary steps could be taken to considerably lessen the impact of the operations to system service/security. | |
| Minimal – 25 | There is little that is likely to be done to substantially mitigate the effect of the threat action and recovery will be prolonged with some permanent effects possible (e.g. loss of data security) | |
| None – 0 | There is no meaningful mitigation or recovery action likely to take place. Recovery will be long and some permanent effects will occur. | |



[redacted]