SAND2019-14000C

# A MATURITY MODEL METHOD FOR NUCLEAR SECURITY PROGRAM ASSESSMENT & PLANNING

L. Dawson
Sandia National Laboratories
Albuquerque, NM
Email: ladawso@sandia.gov

C. Glantz, S. Clements
Pacific Northwest National Laboratory
Richland, WA
Email: cliff.glantz, samuel.clements@pnnl.gov

C. Nickerson
Idaho National Laboratory
Idaho Falls, ID
Email: charles.nickerson@inl.gov

G. White
Lawrence Livermore National Laboratory
Livermore, CA
Email: white6@llnl.gov

**Abstract**

Maturity models of different types have been adopted to help organizations increase capability in a particular discipline by assessing their status relative to a goal, identifying areas where improvement is needed and prioritizing activities to close the gap. There are many examples of maturity models with perhaps to most recognized as the Cybersecurity Capability Maturity Model (C2M2) [1] which was developed by the U.S. Department of Energy to allow organizations in the energy sector to evaluate the programmatic capabilities of their computer security programs in a consistent manner. Such models are critical – indeed any national level capability will be underpinned by strong facility, organizational and individual competency. But, like the C2M2, most models are targeted at the individual facility or organizational level. While necessary, facility-level models are exceedingly detailed and do not facilitate screening assessment and planning at the *National* level.

In response to their mission to lead US international efforts to prevent theft and sabotage of nuclear materials and facilities worldwide, the US Department of Energy International Nuclear Security program has developed a higher-level method appropriate for quickly assessing *nation-level* capabilities and strong translation of that assessment to developing relevant engagement plans and improvement activities. The computer security maturity screening model (CSMS) is designed to provide a rapid preliminary assessment of the relative maturity of a government's nuclear computer security program, including identifying areas of strengths, weaknesses and improvement activities. The method is described below and is prefaced by a common set of terms. The paper will present a computer security example although it is flexible and extensible to any security discipline. When complete such methods facilitate the identification of national needs and could inform the development of an Integrated Nuclear Security Support Plan and incorporating IAEA and other international guidelines for building national nuclear security regimes.

## 1. INTRODUCTION

The consequences of nuclear terrorism represent a grave threat to international security. The responsibility to address the risk of nuclear material theft or sabotage of nuclear facilities is shared by multiple organizations that must strategically collaborate based on their individual missions and capabilities. Stakeholder organizations share a common need to prioritize their activities based on threats, available resources, and existing security program maturity/capabilities, develop engagement plans and measure their progress. However, absent an organizational framework accomplishing this is challenging. Also, compounding the scope of such work is that the nature of improving security touches disparate, complex disciplines. The paper proposes standard terms to help organize the discussion and presents a methodology that will assist selecting long-term risk reduction goals and planning improvement activities across multiple security disciplines and stakeholder organizations. The



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

methodology proposes maturity metrics to assess and communicate performance. The methodology is extensible to any security discipline and a computer security example will be developed for demonstration.

## 2. STANDARD TERMS

***Security Disciplines*** - A nuclear security program is composed of multiple security disciplines. These disciplines include Physical Protection, Material Control & Accounting, Computer security, etc. To improve the security program, it is necessary to evaluate the disciplines individually and prioritize those areas that should have additional resources applied.

***Discipline Domains*** - A domain is a logical grouping of common nuclear security practices that represent a core capability. For example, a core capability for a computer security program is *Incident Response*. A high performing computer security program is prepared for digital failures and cyber attacks, knows who they can rely on for help, how they will isolate the problem and recover the impacted systems. Our process measures, tracks, and communicates improvement in maturity of identified *domains*.

***Maturity Indicators*** - Maturity indicators are the observables that demonstrate security capability for a given domain. For each domain, there are multiple performance indicators to enable an assessment of capabilities. For the incident response example, does the country have an identified organization to help communicate and recover from cyber attacks? Does the country conduct drills and exercises that help them prepare for and assess their capacity to respond to a large scale cyber attack?

***Maturity Levels*** - To simplify communication of goals, maturity indicators can be grouped into levels. Maturity Indicator Levels (MILs) describe a progressive step in a country's capability and/or represent a demonstrated capability for a particular domain. The CSMS model assigns attributes, characteristics, and indicators that represent fundamental capabilities within a domain – Maturity Indicator Levels (MILs).

***Stakeholder Engagement Activities*** - For each domain and maturity level, multi-stakeholder actions are identified based on standards, best practices, or country-specific goals. The stakeholder engagement activities matrix has two important features:

• It organizes across organizations: international organizations, nation state, regulatory agencies, individual organizations, etc. It is not specific to just one organization. Rather it proposes specific actions for all potential stakeholders such as government and regulatory agencies, industry working groups and international organizations. This is an important feature as it represents the breath of potentially available resources and shows how organizations need to collaborate.

• It is based on the maturity level specific to the security discipline and domain. This delivers action plans that correspond to what is needed and can evolve over time as maturity develops.

## 3. COMPUTER SECURITY EXAMPLE

### 3.1. Domains

In the Computer security Discipline, our model requires defining relevant domains. The INS Computer security functional team recommended adopting the domains that were already established by the Nuclear Threat Initiative's Nuclear Security Index [2]. The hope in this selection was to draft on the previous work which had already established priority domains and had collected associated assessment data for many countries.

The NTI index is comprised of the following aspects:

— Mandatory computer security: Do domestic laws, regulations, or licensing rules require nuclear facilities to have protection from a cyberattack?

— Critical digital asset protection: Do domestic laws, regulations, or licensing rules require nuclear facilities to protect critical digital assets from a cyberattack? Critical digital assets include the following systems and networks:

- Safety-related functions
- Security functions
- Emergency preparedness functions
- Support systems and equipment related to the above functions.

— Computer security DBT: Does the state consider cyber threats in its threat assessment or Design Basis Threat (DBT) for nuclear facilities?
— Computer security assessments: Does the regulator require a performance-based program, which includes tests and assessments of computer security at nuclear facilities?
— Cyber incident response plan: Do domestic laws, regulations, or licensing requirements require a cyber-incident response plan for nuclear facilities?

## 3.2. Maturity Indicators

In each domain, individual practices are used to evaluate performance. Practices at Maturity Indicator Level 1 ("MIL1") indicate that the most basic governmental nuclear computer security practices are achieved. MIL1 practices often involve ad hoc activities – activities done by governmental organizations or individual regulators in the absence of detailed laws or regulatory guidance. "MIL2" practices represent a more robust level of governmental performance. These are often associated with documented practices covering the implementation of laws and regulations, the involvement of stakeholders, and adequate resourcing to perform regulatory practices. "MIL3" practices represent the highest level of government performance in the domain. There are often associated with development of detailed policies or directives, reviews for conformance, clearly documented roles and responsibilities, and other more advanced practices.

As a government progresses from one maturity indicator level to the next higher level, it will exhibit a more complete and more advanced implementation of the practices in the domain. Of course, not all governments need to have the most mature nuclear computer security programs. It is anticipated that few, if any, governments will come close to meeting all MIL 1, 2, and 3 practices in all domains. For many governments, particularly for those countries without nuclear facilities, MIL1 performance may be perfectly adequate. Below are practices for each domain, grouped by maturity level.

### 3.2.1. *Mandatory Computer security Requirements*

**MIL1**

- There are some computer security-related requirements (e.g., laws, regulation, policies) established by the government for the nuclear sector, even if these requirements are quite limited in their scope and detail or are an extension of more traditional nuclear security requirements.
- Some nuclear computer security-related implementation guidance is provided by government, or endorsed by government, for use in the nuclear sector.
- There is some government computer security-related oversight at nuclear facilities. Even if computer security is not explicitly listed in inspection criteria, it is examined by some inspectors because computer security is seen as necessary to meet traditional nuclear safety and security requirements.
- There are penalties for failure to comply with some key nuclear computer security-related requirements, even if the penalties are limited in their application or are relatively insignificant (e.g., warnings, small fines).

**MIL2**

- The government has established a set of computer security requirements (in laws, rules, or regulations) that provide a foundation for addressing critical computer security risks at nuclear facilities.
- Nuclear facilities are required to establish and maintain a computer security program.
- Government regulations are consistent with international computer security recommendations and guidance (e.g., from the IAEA, NIST, ISO).
- The government has published guidance to assist its nuclear sector operators in achieving compliance with computer security regulations.
- The competent authority is willing and able to issue meaningful penalties for failure to comply with key computer security requirements.

**MIL3**

- Computer security requirements are integrated with other nuclear security domains including physical security, personnel security, information security, and material control and accountability.

- Computer security-related inspections or assist visits are conducted to assess and aid nuclear facilities in their implementation of measures taken to achieve compliance with computer security requirements.
- The government has a proactive program to review and update regulations and guidance as warranted by the changing computer security environment (e.g., changes in threats and vulnerabilities, development of new security controls).
- The government provides up-to-date technical guidance and support to the industry and sites to reduce computer security risks.

#### 3.2.2. *Critical Asset Protection*

**MIL1**

- Guidance is offered by the government to encourage and assist nuclear facilities in identifying their critical digital assets and systems.
- Guidance is offered by the government to encourage and assist nuclear facilities in protecting their critical digital assets from cyberattacks.

**MIL2**

- Government has established criteria to identify and select critical digital assets and systems (i.e., instructions on how nuclear sites may determine whether an asset or system is "critical" or "non-critical").
- Government requires nuclear facilities to identify their critical digital assets.
- Government provides computer security requirements for critical digital assets.
- The government, either by itself or in conjunction with industry associations, ensures formal training is available to nuclear facility operators to provide instruction on how to identify critical digital assets and systems and how to identify and implement required computer security controls.
- Government requires nuclear facilities to track and document their critical digital assets and the status of all computer security protections (i.e., security controls involving processes, people, and technology) implemented to meet computer security requirements.

**MIL3**

- Government provides nuclear facility operators with tools and techniques for identifying and evaluating the effectiveness of computer security protections for critical digital assets and systems.
- Government inspectors review the identification of critical digital assets and the application of security controls as part of their oversight responsibilities.
- The government requires nuclear facility operators to identify those responsible for conducting and managing the identification of critical digital assets and those responsible for identifying and implementing required security controls.
- The government has a comprehensive set of policies regarding computer security compliance and preferred practices for the computer security of critical digital assets and systems. These policies cover processes, people, and technology.

#### 3.2.3. *Threat and Vulnerability*

**MIL1**

- The government provides guidance to, or endorses guidance for, the nuclear sector on how to incorporate cyber threat information into their computer security program.
- The government shares cyber threat and vulnerability information with the nuclear sector.

**MIL2**

- The government shares threat and vulnerability information with the nuclear sector (i.e., nuclear facilities, contractors, vendors, suppliers, and industry associations) in a timely manner.
- The government shares threat and vulnerability information with the nuclear sector in a structured and secure format.
- Guidance is provided to the nuclear sector on the incorporation of cyber threat capabilities into a design basis threat.

**MIL3**

- The government has established a dedicated national organization (e.g., an Information Sharing and Analysis Center) that is tasked with sharing vulnerability and threat information within the nuclear sector (though it may support other sectors as well).
- The government performs a periodic technical review of the design basis threat assessment produced by each nuclear facility and the security controls implemented to address the design basis threat.

#### 3.2.4. *Inspections and Assessments*

**MIL1**

- The government has a program to inspect security at nuclear facilities and this inspection includes at least some elements of computer security.

**MIL2**

- Inspections are conducted to verify compliance with the computer security requirements issued by the government (e.g., as laws, rules, regulations).
- Computer security inspection guidelines and procedures are documented for use by the competent authority's inspectors.
- Inspections seek to verify that the nuclear facility operator is following the facility's own documented computer security plan (including policies and procedures).
- The inspection-related enforcement process is defined. This includes penalties for non-compliance.
- Adequate resources are provided by the government to support their computer security inspection program (e.g., budget, staff, time to perform assessments).

**MIL3**

- Computer security inspections by the competent authority are governed by laws and regulations.
- The competent authority's computer security inspectors have clearly defined responsibilities and clear authority to perform detailed inspections of nuclear facilities.
- The competent authority's computer security inspectors have appropriate knowledge and training to perform their inspection duties. This includes appropriate computer security technical expertise.
- The government interacts with international organizations and industry associations to identify and implement improvements in its computer security inspection program.
- Requirements for computer security self-assessments by nuclear facility operators are governed by laws and regulations.

#### 3.2.5. *Incident Response*

**MIL1**

- The government has a designated entity/office/position to receive computer security event reports.
- The government tracks computer security event reports and the response of nuclear facility operators to computer security events.
- The government analyses computer security events, even if only in an ad hoc manner, in order to appropriately characterize the event and provide information to nuclear facility operators that may be at risk.
- The government has identified computer security support personnel, even if only in an ad hoc manner, who can assist the government and industry in addressing a significant computer security event.

**MIL2**

- The government maintains an official repository (e.g., database) for logging "escalated" (i.e., unusual or of elevated risk) computer security events.
- The government establishes criteria for nuclear facilities to support their development and maintenance of computer security event detection (e.g., what constitutes an event, where to look for events), analysis, and response capabilities.
- The government maintains a capacity to provide timely assistance to nuclear facilities that are experiencing a computer security event that could adversely impact safety, security, or emergency response systems or functions.
- Adequate resources are available to receive reports of computer security events, track these events, and provide assistance to impacted facilities.

- Standards and/or guidelines have been identified and are used to inform the government's response to a computer security event.

**MIL3**

- The competent authority maintains a policy and procedures for reporting computer security event and incident information to designated authorities (e.g., other government and international agencies) in conformance with applicable laws, regulations, and agreements.
- Escalated computer security events are correlated by the competent authority to support the discovery of patterns, trends, and other common features.
- The government provides requirements or guidance for nuclear facility operators on maintaining continuity and prompt restoration of safety, security, and emergency response functions in the wake of a computer security event.
- Personnel performing computer security event and incident response duties have the skills and knowledge needed to perform their assigned responsibilities.

### 3.3. Maturity Levels

Table 1 lists the number of practices the model provides in each domain.

TABLE 1. DOMAIN PRACTICES

| Domains | Number of Initial Practices (MIL1) | Number of More Mature Practices (MIL2) | Number of Highest Maturity Practices (MIL3) | **Total Practices by Domain** |
|---|---|---|---|---|
| Mandatory Computer security | 4 | 5 | 4 | 13 |
| Critical Asset Protection | 2 | 5 | 4 | 11 |
| Threat and Vulnerability | 2 | 3 | 2 | 7 |
| Inspections & Assessments | 1 | 5 | 5 | 11 |
| Incident Response | 4 | 5 | 4 | 13 |
| Totals at Each MIL Level | 13 | 23 | 19 | 55 |

Within a given domain, maturity levels are described from across a spectrum from absent to fully mature. Each practice is evaluated using a four-level scoring system, as outlined in Table 2 and graded as either Fully Implemented (FI), Largely Implemented (LI), Partly Implemented (PI), or Not Implemented (NI).

TABLE 2. COMPUTER SECURITY MATURITY LEVELS

| Implementation Level | Definition |
|---|---|
| NI | Not Implemented - Absent |
| PI | Partially Implemented – Incomplete; there are multiple opportunities for improvement |
| LI | Largely implemented - Complete, but with recognized opportunity for improvement |
| FI | Fully implemented - Complete |

When determining the overall maturity level of a government’s nuclear computer security program within a domain, all the MIL1 practices in a domain must be achieved at the fully or largely implemented level to achieve an overall MIL1 designation for that domain. If even one practice at the MIL1 is partly or not implemented, MIL1 is not achieved and the overall maturity level for the domain is designated as “MIL0”. All the MIL1 and MIL2 practices must be achieved at the fully or largely implemented level in a domain to achieve an overall MIL2

designation for that domain. Similarly, all the MIL1, MIL2, and MIL3 practices must be achieved at the fully or largely implemented level in a domain to achieve an overall MIL3 designation for that domain.

### 3.4. Evaluating the Results of the Assessment

The following eight-step process can be followed to evaluate the results of the assessment:

Step 1. After recording the fully, largely, partly, or not implemented scores for each practice in each domain, turn your attention back to the first domain.

Step 2. Look at the evaluation scores for the MIL1 practices. If all the MIL1 practices are fully or largely implemented, then MIL1 is achieved for that domain. If not, the domain is at MIL0.

Step 3. If MIL1 is achieved for the domain, look at the evaluation scores for the MIL2 practices. If all the MIL2 practices are fully or largely implemented, then MIL2 is achieved for that domain.

Step 4. If MIL2 is achieved, look at the evaluation scores for the MIL3 practices. If all the MIL3 practices are fully or largely implemented, then MIL3 is achieved for that domain.

Step 5. Repeat Steps 2-4 for the remaining four domains.

Step 6. After this is completed, you will have a MIL for each of the five domains. This supports the identification of domains that have higher and lower maturity levels for the government's nuclear computer security program. In some cases, all domains may have the same maturity level.

Step 7. The overall maturity level for the government's nuclear computer security program is the lowest MIL level in any domain. As a result, a small improvement in a single practice in the domain with the lowest MIL could increase the MIL score for the entire governmental program.

Step 8. Implementation scores for individual practices can be evaluated to identify any practices for which cost effective assistance could potentially be provided to improve the maturity of the assessed government's nuclear computer security program.

Figures 1 and 2 present example displays of the output from the application of Steps 1-6. Figure 1 presents an outcome where there is a large disparity between the performance in the five domains. While only one domain is at MIL0 and the other domains achieve, MIL1, MIL2, or MIL3, the overall maturity level for the government is MIL0 because one domain has an extremely low maturity. Domains with higher maturity levels are positive features, but the overall performance of that government's nuclear computer security program is handcuffed by the low maturity in one domain.

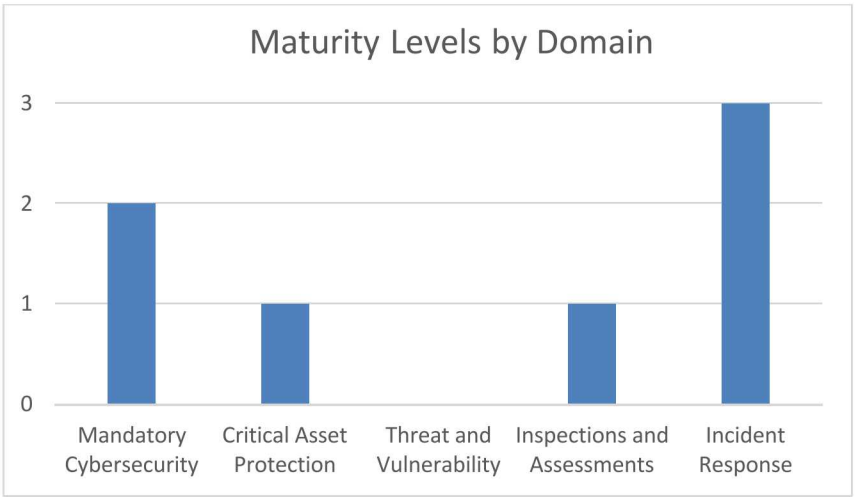


***Figure 1***. *An initial evaluation of the maturity levels in each domain. The overall maturity level is at MIL0 because the domain with the lowest maturity level does not achieve MIL1.*

Figure 2 presents one way a government could balance out its nuclear computer security performance (as originally displayed in Figure 2) without increasing expenditures. In this figure, the government has transferred resources from the domain formerly achieving MIL3 to address deficiencies in the domain that was not achieving MIL1. Now all domains have at least a MIL1 score and so the overall maturity level is at MIL1.

While reallocating nuclear computer security resources may not be the optimal solution, it may be the most economical option in situations where new resources are not available.

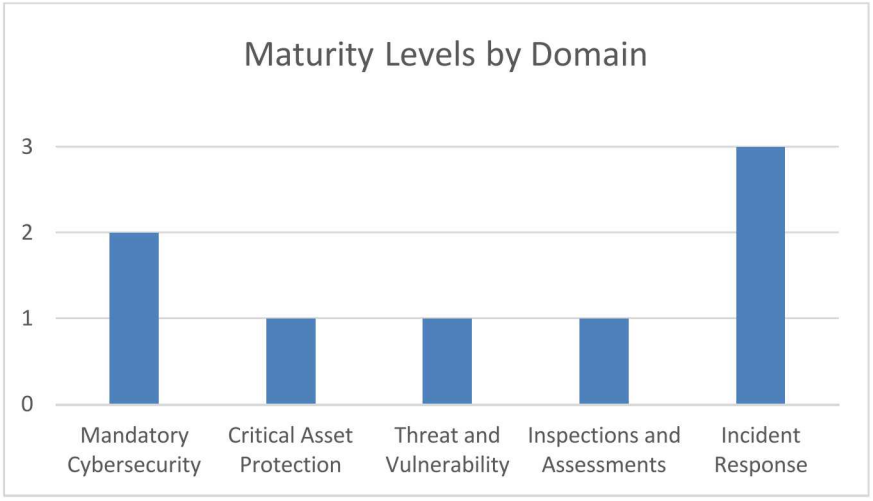


***Figure 2.*** *A revised evaluation of the maturity levels in each domain after the government redeploys resources to achieve an overall maturity level of MIL1.*

### *3.5.* Stakeholder Engagement Activities

The assessment activities above will yield domains that are immature and security practices that are absent. An important next step is to plan specific activities to improve the situation. The absent best pratices become places where improvement is indicated. When fully realized, the method will include stakeholder engagement activities which will correspond to the evaluated maturity level and help engage a full spectrum of possible stakeholders. Table 3 is an example of potential stakeholder engagement activities that could be incorporated into a improvement plan.

TABLE 3. EXAMPLE STAKEHOLDER ENGAGEMENT ACTIVITIES

| | | | **Stakeholders** | | | |
|---|---|---|---|---|---|---|
| | | | **INS** | **Government and Regulators** | **Nuclear Industry** | **International Organizations** |
| **Maturity Levels** | **All** | | Promote research - ICS w/ enhanced IDS, defense-in-depth, recovery, etc. | Invest in human capacity, R&D, awareness and inter-national collaboration | Field systems with enhanced IDS and recovery | Promote Incident Response Plan (IRP) sharing and regional exercises. |
| | **3** | Country has documented IRP and conducts exercises | | Continue existing programs, apply lessons learned from cyber event exercises | | |
| | **2** | Country has documented IRP | | Develop exercise scenarios and plans | | Best Practice Sharing |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **1** | Country organizations exist to help facilities with cyber event. | New class helping countries and facilities develop IRPs | Develop IRP, training, expert solicitation | | Share existing country-level IRPs |
| | **0** | No evidence IRP exists or used | Cyber Basics class emphasizing the evolving threat | Establish country-level capability to organize cyber event IRP | Characterize facility systems. Develop facility-level IRPs | |

## 4. CONCLUSIONS AND NEXT STEPS

The paper has presented a common set of terms and a method for assessing nation-level security capabilities and developing relevant engagement plans and improvement activities. The method was presented with a cyber security exemplar but is readily translatable to any security discipline. When complete such methods facilitate the identification of national needs and could inform the development of an Integrated Nuclear Security Support Plan and incorporating IAEA and other international guidelines for building national nuclear security regimes. Currently the DOE INS is looking to partner with other countries to vet the method and start engagements to understand and improve nuclear cyber security.

## REFERENCES

[1] U.S Department of Energy, 2014a. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Version 1.1 http://energy.gov/node/369271

[2] Nuclear Threat Initiative (NTI) Nuclear Security Index "Building a Framework for Assurance, Accountability, and Action, Fourth Edition, September 2018. https://ntiindex.org/wp-content/uploads/2018/08/NTI_2018-Index_FINAL.pdf

## ACKNOWLEGMENTS

*Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.*