Department of Homeland Security

Cybersecurity Capability Maturity Model White Paper

Version 1.0

August 4, 2014

Executive Summary

Cybersecurity is a leading national security challenge facing this country today. An emerging topic of importance is how organizations track, assess, grow, and shape their workforce. Many organizations have turned to workforce planning as a way to understand their current cybersecurity human capital skills and abilities as well as potential infrastructure needs.

The National Initiative for Cybersecurity Education (NICE) evolved from the Comprehensive National Cybersecurity Initiative (CNCI), Initiative 8 - Expand Cyber Education, to develop a technologically-skilled and cyber-savvy workforce with the right knowledge and skills. Towards these ends, Component 3 of NICE is focused on the cybersecurity Workforce Structure — specifically talent management and the role of workforce planning in developing the national cybersecurity workforce. NICE has initiated discussions and issued guidance on workforce planning for cybersecurity best practices. In spring 2012, NICE published a white paper titled: *Best Practices for Planning a Cybersecurity Workforce*[1], which introduces workforce planning methodologies for cybersecurity. This White Paper introduces a qualitative management tool, a Cybersecurity Workforce Planning Capability Maturity Model, to help organizations apply the best practice elements of workforce planning in analyzing their cybersecurity workforce requirements and needs.

The NICE Capability Maturity Model

As the cybersecurity workforce continues to evolve and organizations track and manage against the changing cybersecurity environment, understanding where current workforce planning capabilities lie and how to further develop has become increasingly important.

A capability maturity model (CMM) provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning, establishing a foundation for consistent evaluation. It allows organizations to compare their capabilities to one another, and enables leaders to make better, well-informed decisions about how to support progression and what investments to make in regard to cybersecurity human capital initiatives.

This White Paper defines NICE's CMM by segmenting key activities into three main areas: 1.) process and analytics, 2.) integrated governance, and 3.) skilled practitioners and enabling technology.

- ***Process*** represents those activities associated with the actual steps an organization takes to perform workforce planning and how those steps are integrated with other important business processes throughout the organization. ***Analytics*** represents those activities associated with supply and demand data and the use of tools, models, and methods to perform workforce planning analysis
- ***Integrated governance*** represents those activities associated with establishing governance structures, developing and providing guidance, and driving decision-making. It is the building block to an organization's overall workforce planning strategy and vision as well as assignments of responsibility, promotion of integration, and issuing of planning guidance
- ***Skilled Practitioners*** represents the activities associated with establishing a professional cadre of workforce planners within an organization. ***Enabling Technology*** represents the activities associated with the accessibility and use of data systems

[1] Cybersecurity Education Office, National Initiative for Cybersecurity Education (2012). *Best Practices for Planning a Cybersecurity Workforce White Paper*.

Using the NICE CMM

The NICE Cybersecurity Workforce Planning CMM has three maturity levels. These levels are ***limited, progressing, and optimizing***. Limited is the most basic level, portraying a key activity area or segment of an organization's cybersecurity workforce planning capability that is in its infancy. This level of capability is at its start of development and may be represented by an organization having limited establishment of processes, lacking clear guidance, or having little in terms of data and analysis methods. The progressing level describes a key activity area of some aspect of cybersecurity workforce planning which an organization has started to perform, commonly represented by an organization establishing some infrastructure to support workforce planning efforts. The final level of maturity, optimizing, depicts a key activity area or segment of cybersecurity workforce planning capability that has fully developed, such as one that is integrated with other business processes and can support different levels of workforce and workload analysis, the results of which drive short- and long-term decision making for the cybersecurity workforce.

It is important to note that organizations will have differing goals when it comes to the maturation of the cybersecurity workforce planning capability and that all organizations do not need to reach the optimizing state for all key areas. Organizational goals should take into account many different variables. Leaders need to assess the impacts of: allocation of resources, implementation, timing, and return on their investments. Therefore, organizations should view their maturity rankings less as a grade or judgment and more as an indication of resources spent on workforce planning. Having a "limited" maturity level does not equate to "bad" workforce planning, but rather that the organization has not dedicated resources to partially or fully develop that aspect of the maturity model, and that there are extenuating circumstances for that outcome.

In order to use the model, organizations must have an accurate understanding of their current workforce planning capabilities as they relate to the three segment areas, with the ability to cite specific evidence of conducting related activities. An organization's current capability is the springboard upon which to build further maturity, using the CMM to pinpoint necessary next steps and decision points for progression. NICE recommends a three-step process to using the CMM to determine an organization's current cybersecurity workforce planning capability and progress individual organizational maturity along the continuum:

1. Gather data on qualitative CMM variables
2. Analyze data and determine current maturity levels by CMM key area
3. Determine priority areas for increased maturity and develop action plans

Benefits

No matter an organization's maturity level, it can realize several benefits by practicing good cybersecurity workforce planning. These benefits include, but are not limited to:

- Increased consistency in execution of organization-wide cybersecurity workforce planning activities
- Enhanced data-driven decision making and analysis around shaping, building, growing, and supporting a cybersecurity workforce
- Enhanced confidence and credibility from the field in headquarter decisions and guidance on cybersecurity workforce planning
- Decreased response times to analysis requests and external reporting requirements, enabling timely and proactive decisions to modify or change cybersecurity workforce policy as needed

- Increased organizational alignment and pragmatic solution development between workforce, human capital, budget, and strategic planning organization sections or departments

Next Steps

The next steps following the application of this CMM, and the Component 3 Workforce Planning Project, are currently under development.

Table of Contents

EXECUTIVE SUMMARY **II**

THE CYBERSECURITY LANDSCAPE: NOW'S THE TIME TO PLAN **1**

MAKING THE CASE: A NEED FOR CYBER WORKFORCE PLANNING CAPABILITY **1**

The Practice of Workforce Planning 2

The Benefits of Workforce Planning 2

INTRODUCTION TO THE NICE CMM **3**

DEFINING WORKFORCE CMMS **4**

Existing Models 4

Components of the NICE CMM 5

CRITERIA AREAS 5

MATURITY LEVELS 7

DETAILED OVERVIEW OF THE NICE CMM **8**

Process and Analytics 8

INTEGRATED GOVERNANCE 10

Skilled Practitioners and Enabling Technology 12

ACHIEVING MATURITY **15**

Differing Maturity Goals 15

Assessing Current Capability 15

Step One: Gather Data 15

Step Two: Analyze Data and Determine Current Maturity 16

Step Three: Progressing in Maturity 17

BENEFITS OF ACHIEVING CYBERSECURITY WORKFORCE PLANNING MATURITY **18**

CONCLUSION **19**

APPENDIX A. BEST PRACTICES FOR PLANNING A CYBERSECURITY WORKFORCE COMPONENTS **A-1**

APPENDIX B. PROCESS DEFINED **B-1**

APPENDIX C. GOVERNANCE STRUCTURE DEFINED **C-1**

APPENDIX D. NICE CMM **D-1**

APPENDIX E. ACRONYM LIST **E-1**

The Cybersecurity Landscape: Now's the Time to Plan

The President of the United States, Congress, and leaders of Executive Agencies have identified Cybersecurity as one of the leading national security challenges facing this country. As a result, the policies and programs that currently exist in regard to the cybersecurity workforce have come under much scrutiny. Specifically, an emerging topic of importance is how organizations track, assess, grow, and shape this workforce. Many organizations have turned to workforce planning as a way to understand their current cybersecurity human capital skills and abilities as well as potential infrastructure needs.

Workforce planning is a systematic way for organizations to determine the current and future human capital requirements (demand), identify current human capital capabilities (supply), and design and implement strategies to transition the current workforce to the desired future workforce.[2] It supports organizations by systematically identifying cyber professionals, in standardized terms, to accurately account for the current workforce. It identifies and quantifies the workload and workforce requirements unique to the organization; and analyzes the skills and talent needed to fill the gap in workforce. Good workforce planning is designed in a repeatable and reliable fashion, highlighting risks and forecasting needs over time.

> *"Cyber threat will pose the number one threat to our country…Intrusion into corporate networks, personal computers, and government systems are occurring every single day, and they threaten our economy and our way of life…Now we must position ourselves to best combat the cyber threat as it grows and morphs over the next 10 years…This is the threat of the futures We're doing everything possible to ensure that we have the organizational structure, expertise, and capabilities to stay one step ahead of the adversary."*
> *--FBI Director Muller*

The National Initiative for Cybersecurity Education (NICE) evolved from the Comprehensive National Cybersecurity Initiative (CNCI), Initiative 8 - Expand Cyber Education, to develop a technologically-skilled and cyber-savvy workforce with the right knowledge and skills. Towards these ends, Component 3 of NICE is focused on the Cybersecurity Workforce Structure — specifically talent management and the role of workforce planning in developing the national cybersecurity workforce. NICE has initiated discussions and issued guidance on workforce planning for cybersecurity best practices. In spring 2012, NICE published a White Paper titled: *Best Practices for Planning a Cybersecurity Workforce*, which introduces workforce planning methodologies for cybersecurity. This companion White Paper introduces a qualitative management tool, a Cybersecurity Workforce Planning Capability Maturity Model (CMM), to help organizations apply the elements of best practice workforce planning to analyze their cybersecurity requirements and maturity needs.

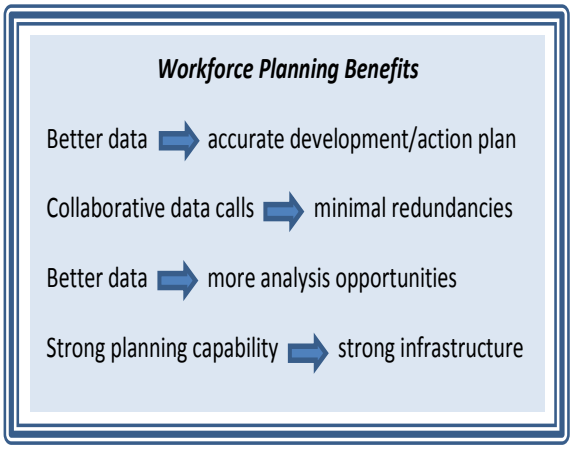
Making the Case: A Need for Cyber Workforce Planning Capability

Organizations across the Federal, state, local, tribal and territorial governments, industry, and academia all have varying maturity levels of cybersecurity workforce planning capabilities. However, despite differences across sectors, there are several common characteristics and realized benefits from practicing good workforce planning.

[2] "Strategic Planning: The Strategy behind "Strategic Staffing." Christina Morfeld. http://capsnet.usc.edu/ProfessionalDevelopment/SupportTools/documents/StrategyBehindStrategicStaffing.pdf

The Practice of Workforce Planning

An organization practicing good workforce planning has aligned its process to other organizational business processes. It has a common language and taxonomy to define cybersecurity workforce needs and can make adjustments based on workforce changes and demand. These adjustments allow the organization's cybersecurity personnel to be highly agile in responding to emerging technology and new threats. A central source or department hosts the process for the cybersecurity workforce, providing support, offering clarifying guidance, developing tools, and performing analysis to determine overall, cross-cutting workforce trends in cybersecurity for the organization. Host leaders recognize that the sub-organizations possess knowledge that is not available to headquarters, and support the gathering of cybersecurity workforce data at a sub-organization level to provide more effective supply and demand analysis gathered from sources charged to execute the actual work. Together, leaders and practitioners drive the tactical implementation of a documented, communicated, and consistent process, ensuring integration within the strategic, budget and human capital planning cycles. Sub-organizations and headquarters are also consistent in sharing information as well as leveraging the same types of data, using established systems which gather, store, and aid in analysis of supply and demand data. These optimal systems are user-friendly, accessible, and provide enough breadth to aid users in gaining a complete picture of the entire workforce. Simply put, workforce planning enables an organization to forecast, with confidence, what the future demand looks like and easily pinpoint areas of current and future risk. In turn, the organization uses this analysis to drive short- and long-term decision making.



The Benefits of Workforce Planning

In recent years, cyber-attacks have grown in sophistication and reach. These attacks have become a national leadership priority spanning from Congress to the President. Our nation's best defense to these emerging threats is to develop a robust, agile, and highly trained cybersecurity workforce. However, to build this workforce, organizations must have an understanding of their current supply as well as approaches to identify and meet future demand. An organization with a mature cybersecurity workforce planning capability has this information, enabling its leaders to make proactive, defensible, and data-driven decisions about cyber personnel and their work. For example, understanding current capabilities and how the demand for these capabilities will change based on emerging cyber threats enables organizational leaders to make better decisions in regard to the types of training needed to develop their cybersecurity professionals or how to target recruiting efforts to ensure that the organization has the right cybersecurity skills to meet future demands.

In addition, because an organization with a mature workforce planning capability has access to better data and information, it is able to develop action plans to minimize gaps between workforce supply and workload demand. For example, if an organization employs sophisticated models or tools to analyze a complete set of supply data to understand its cybersecurity workforce's separations, attrition, and promotion rates and pairs that information with other data such as engagement scores, it can identify overall retention issues and their root causes. Further, the

organization understands the impact of attrition to the organization and can develop action plans that prevent and preempt further separations resulting in less supply and demand gaps.

Finally, this capability allows an organization to minimize redundancies of effort because data calls are at a minimum and key players are in constant contact.

These benefits are especially important to cybersecurity because the workforce is dynamic, requiring that an organization be able to make timely decisions and quickly take actions to account for the changing need of cybersecurity workers and related work. Moreover, because of the criticality of cybersecurity and its rate of growth, strong data on the cybersecurity workforce is also required to deploy prompt solutions and pragmatic action plans. Simply stated, organizations' leaders make better investments, human capital or otherwise, when they have data in hand and can fully assess the consequences and impacts of their decisions.

In addition to these advantages, a unique benefit gained by an organization practicing good workforce planning is the strengthened ability to analyze the workforce in unconventional ways and develop innovative solutions. For example, an organization might find that there is a concentration of cyber intrusion attacks within one specific office's area of responsibility (AOR), and that the current cybersecurity workforce in that office is insufficient to cover the increased workload. Good workforce planning also provides the organization with the knowledge that the workload in another AOR has decreased in recent times. Consequently, because cybersecurity work is highly mobile, the organization can "move" the overflow work to the other AOR to establish appropriate coverage. Innovation and quick response are two success factors of any cybersecurity workforce. Therefore, workforce planning can lead to faster reaction time, stronger solutions, and greater overall success for the cybersecurity workforce and organization.

Finally, the cybersecurity workforce does not only fall within one division of an organization - cybersecurity is a part of every position that touches technology. As a result, there is an increased demand for individuals that have cyber skills, but who are not necessarily 100% aligned to the cybersecurity workforce. It is important for organizations to have a mechanism by which they can compare the workforce that performs all aspects of cybersecurity duties. Workforce planning is a consistent way of analysis and a process which affords a comparison between very different sub-organizations to enable an organization to have the appropriate infrastructure in place as the workforce matures.

Introduction to the NICE CMM

Much like the cybersecurity workforce, most organizations' cybersecurity workforce planning is still in its infancy. Therefore, before substantive improvements can be made, organizations must assess their requirements against a mature workforce planning capability.

A defined CMM provides a structure for organizations to baseline their capability, establishing the foundation for consistent evaluation for those organizations with small, medium, and large sized cybersecurity workforces. Additionally, a CMM allows organizations to compare their capabilities to one another because they all use the same criteria from which to work. This ability enables leaders to make better decisions about how to support progression and to make inform decisions around what investments to make in regard to cybersecurity human capital initiatives.

This White Paper provides an introduction to the NICE proposed CMM. It defines NICE's CMM by segmenting key activities into three main areas: 1.) ***process and analytics***, 2.) ***integrated governance***, and 3.) ***skilled practitioners and enabling technology***, with three levels of maturity - limited or progressing or optimizing.

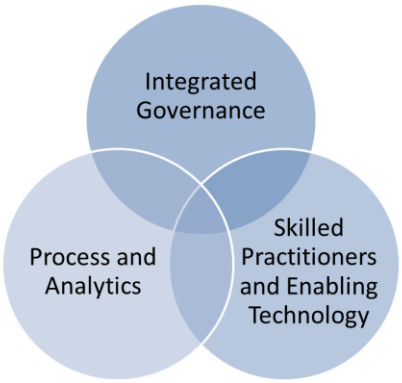


Figure 1. NICE CMM Areas

This White Paper also describes the three levels of maturity in regard to process and analytics, integrated governance, and skilled practitioners and enabling technology, and provides corresponding activities and example evidence of development of a cybersecurity workforce planning capability. Finally, this White Paper discusses the benefits of building out a workforce planning capability, and how an organization might progress along the CMM - including situations where organizations may not always pursue an "optimizing" rating. This information will enable organizations to quickly pinpoint where they are in terms of developing their cyber workforce planning capability and next steps.

Defining Workforce CMMs

A CMM is a construct that defines different levels of maturity across a workforce planning development spectrum. The maturity levels are segmented into definitive groups that build upon one another and are easily distinguishable. For the purpose of this White Paper, maturity relates to how optimized cybersecurity workforce planning is at an organization. As an organization moves along the spectrum, it is making progress in developing the evaluated capability.

A CMM uses a qualitative data gathering process to identify inputs and determine outputs. It is a management tool that aids leadership in identifying opportunities for future growth and evolution of an organization's cybersecurity workforce planning capability. It is not a quantitative tool or model that allows for a calculation of a numerical "score" of maturity or an exhaustive listing of all current workforce planning practices, tools and resources employed at an organization. Moreover, it is neither a "scorecard" nor a "report card", and it should not be used as a punitive assessment. Instead, its focus is on the fundamental building blocks of a capability. A CMM helps organizations establish where they are, for better or worse, on the maturity spectrum, and determine where to grow from there. A CMM helps clearly depict where organizations currently reside in the development of this specific capability, and where they will need to focus future resources to mature.

Existing Models

There are many existing maturity models in use across the workforce planning arena. NICE researched three available models (noted below in figure 2). The analysis revealed that there are some commonalities, but that there are many ways in which various entities approach workforce planning maturity. Table 1 below outlines the key points about each of the researched CMMs.

Table 1. Examples of Existing CMMs[3][4][5]

Org.	Maturity Levels	Key Components
The Newman Group	Basic, Intermediate	• Matrix of value delivered to the organization and data analysis required • Basic level: understanding current workforce through simple metrics like headcount • Intermediate level: performing projections and gap analysis, segmenting the workforce
Talent Strategy Advisors	Cautiously Tactical, Soundly Operational, Passionately Optimistic	• Evaluation categories of: intent, resources, planning and control, interventions • Cautiously Tactical: centralized, HR driven initiative focused on critical positions • Soundly Operational: strategic initiative with some integration between HR and business units focused on critical positions and their supervisors • Passionately Optimistic: decentralized, fully integrated, strategic initiative focused on critical positions, supervisors, and managers
Infohrm	Beginning, Intermediate, Advanced	• Evaluation categories of: key focus, team, data, software, tools, processes, integration, forecast demand, and business information • Beginning: inconsistent process with ad hoc use of tools and data systems, and HR needs • Intermediate: consistent process using business unit data, drives demand forecasting • Advanced: established Center of Excellence that provides tools and supports a consistent process that is tied to business planning, drives overall business strategy

All of the CMMs reviewed for this White Paper have levels of maturity with associated activities. However, a segmented process to capability development is where the similarities end. Each model focuses on different variables, which highlights the fact that there is no single best approach to assess workforce planning maturity, but rather a customized approach, relevant to the specific workforce and organization, is optimal. Therefore, NICE leveraged the structure and foundational principles of each CMM to develop the NICE cybersecurity CMM.

Components of the NICE CMM

Criteria Areas

As previously mentioned, the NICE CMM has three areas that link to the three components of workforce planning practices introduced in the *Best Practices for Planning a Cybersecurity Workforce White Paper*[6]. As shown in Figure 2 below, the Process and Analytics area relates to the Process component, the Integrated Governance area of the CMM correlates with the Strategy component, and the Skilled Practitioners and Enabling Technology relates to the Infrastructure component.

---

3 "Workforce Planning: Achieve Talent Management Success." The Newman Group: A Futurestep Company. April 2009. Available at www.tng.futurestep.com

4 "Workforce Planning Maturity Model: a tool for improving an organization's strategic capability." Talent Strategy Advisors. March 23, 2010. Available at www.talentstrategyadvisors.com

5 "Infohrm's Workforce Planning Maturity Model: Three levels of increasing workforce planning sophistication."Infohrm. Available at www.infohrm.com or through www.apqc.org

6 Cybersecurity Education Office, National Initiative for Cybersecurity Education (2012). *Best Practices for Planning a Cybersecurity Workforce White Paper.*

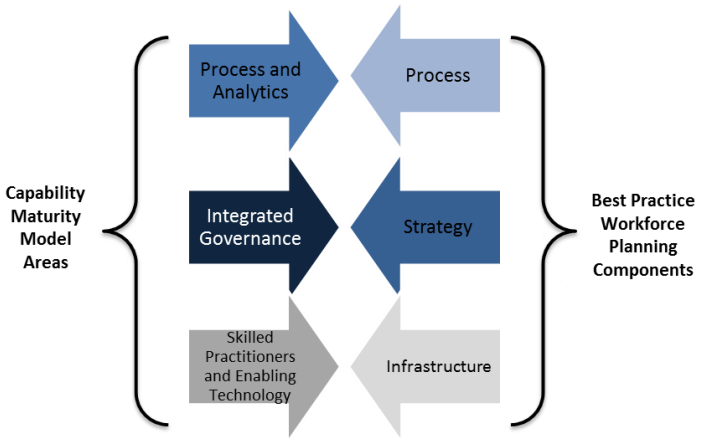


Figure 2. CMM and Components Relationship[7]

Additionally, the *Best Practices for Planning a Cybersecurity Workforce White Paper* identified the unique workload and workforce requirements of cybersecurity affecting supply and demand in workforce planning. These requirements also influence the development of the cybersecurity workforce planning CMM components. These requirements are:

Workload Requirements:

- ***Surge Capacity*** *– the need to expand resources and capabilities in response to prolonged demand*
- ***Fast-paced*** *– the need to sustain multiple workstreams occurring rapidly*
- ***Transformative*** *– the need to adapt to fundamental changes to technology, processes, and threats*
- ***High Complexity*** *– the need to employ a large number of intricate technologies and concepts*

Workforce Requirements:

- ***Agile*** *– the ability to shift between roles or needs should a threat warrant different support*
- ***Multi-functional*** *– the ability to maintain and execute a variety of activities at any given time*
- ***Dynamic*** *– the ability to provide for constant learning to effectively approach new endeavors and problems*
- ***Flexible*** *– the ability to move into new roles or environments quickly to increase knowledge and skills*
- ***Informal*** *– the ability to work in a nontraditional environment*

These requirements provide an initial baseline of characteristics that leaders and practitioners will need to track, assess, and manage against in order to accurately capture the workforce's current composition and project its future state. For example, a workforce that has stable demand and predictable schedules, or has requirements that dictate a number of personnel per work task, has a set demand. As such, sophisticated demand tools or templates are not necessary to project the future state of the workforce. Therefore, unlike the NICE Cybersecurity CMM, a CMM evaluating workforce planning for that type of workforce segment would have little emphasis on demand tools or analytics.

[7] For further explanation of the three Best Practices for Planning a Cybersecurity Workforce components, see Appendix A.

Table 2 crosswalks the CMM area component to the cybersecurity workload and workforce requirements. Please note, that it is possible for a requirement to appear in more than one capability criteria because one component area encompasses many factors.

Table 2. CMM Criteria and Requirements Crosswalk

CMM Capability Criteria	Requirements
Process and Analytics	• Surge • Transformative • Agile • Flexible
Integrated Governance	• Fast-paced • Transformative • Multi-functional
Skilled Practitioners and Enabling Technology	• Surge • Fast-paced • High complexity • Dynamic • Flexible

Cybersecurity workload has surges and the workforce must be agile and flexible. As such, there is not a set demand for the cybersecurity workforce. There is a need for multiple demand tools, templates, and models in order to perform a thorough analysis. Consequently, the NICE CMM has a section within the process and an analytics capability area that allows for evaluation on the existence and use of tools, methods, and models to aid in planning.

Additionally, the cybersecurity workforce is still evolving and the structures to manage its development are relatively new and not fully established. The cybersecurity discipline is fast-paced, transformative, and multi-functional. Due to the relative recent emergence of cybersecurity, it is important for organizations to set the vision, strategy, and governance roles for their cybersecurity workforce planning capability as a foundation for growth. This is addressed in the NICE CMM through the inclusion of integrated governance as one capability area.

Finally, because the cybersecurity workforce is focused on technology, and the nature of the work is highly complex and dynamic, a component within the CMM that encompassed the use of data through skilled practitioners and enabling technology has been introduced. Additionally, since cybersecurity professionals are often distributed throughout a wide array of departments in any larger organization; gathering, storing, and analyzing data via shared tools is a better and more efficient use of workforce practitioner's time.

Maturity Levels

Lastly, the NICE Cybersecurity Workforce Planning CMM has three maturity levels. These levels are limited, progressing, and optimizing (see Figure 3). Limited is the most basic level, portraying an organization with areas of its cybersecurity workforce planning capability in its infancy. This key area of the organization is at the beginning of its development, for example having limited establishment of processes, lacking clear guidance, and having little in terms of data and analysis methods. The progressing level describes some aspects of cybersecurity workforce planning throughout the organization that have started to perform and establish some infrastructure to support efforts. The final level of maturity, optimizing, depicts key areas of

Figure 3. Maturity Levels

workforce planning capabilities in an organization that are fully developed, are integrated with other business processes, and can support different levels of workforce and workload analysis, the results of which drive short- and long-term decision making for the cybersecurity workforce.

Detailed Overview of the NICE CMM

As previously stated, the NICE CMM segments key activities of cybersecurity workforce planning into three main areas: 1.) process and analytics, 2.) integrated governance, and 3.) skilled practitioners and enabling technology. Each of these three areas has specific associated activities to gain maturity through three levels, which build upon each other – limited, progressing, and optimizing. Working together, these three area segments evaluate an organization's overall cybersecurity workforce planning capability. In order to use the NICE CMM, organizations must have an accurate understanding of their current workforce planning capabilities as they relate to the three segments, with the ability to cite specific evidence of examples of activities they conduct. Their current capability will be the springboard upon which they build further maturity, using the CMM to pinpoint next steps and decision points for progression.

The following section provides a detailed overview of these segments.

Process and Analytics

Process represents those activities associated with the actual steps the organization takes to perform workforce planning and how those steps are integrated with other important business processes throughout the organization. ***Analytics*** represents those activities associated with supply and demand data and the use of tools, models, and methods to perform workforce planning analysis.

Process includes activities, *or efforts,* that focus on the integration of the workforce planning process with other business planning processes. This area also measures how the process influences decision making as well as how leaders monitor the overall performance of the workforce planning process. This section is especially important to the cybersecurity workforce because of its priority status: leaders will continue to divert resources to support cybersecurity and it is essential that these connections are understood so decisions are consistent and accepted across the organization.

The *Best Practices for Planning a Cybersecurity Workforce White Paper* discussed the steps of a best practice workforce planning *process*[8]. For the purpose of this paper, process and the term *efforts* are interchangeable and include the below steps:

1. Conducting an inventory of an organization's current workforce (e.g., skills, capabilities)
2. Performing a supply and demand analysis
3. Executing a gap analysis
4. Developing an implementation plan

Analytics includes the existence and characteristics of supply and demand data as well as the presence and use of workforce planning tools, models, and templates. Since cybersecurity is so unique, the developed CMM accounts for the way in which organizations should consider, use, and analyze its supply and demand data to drive decisions and inform planning.

[8] The "process" is defined by the to two best practice processes (i.e., Federal and private sectors) in the *Best Practices for Workforce Planning White Paper* and explained further in Appendix B.

The *Best Practices for Planning a Cybersecurity Workforce White Paper* discussed *analytic* factors in terms of performing risk assessments and using customized tools. Similarly, the NICE Cybersecurity Workforce Planning CMM describes analytics in terms of analysis tools, templates, and methods as well as the existence and usability of supply and demand data. Therefore, the CMM and Best Practices link together in the following way:

1. Examining potential risks[9] to an organization's workforce development process
2. Considering mitigation solutions
3. Developing and employing customizable analytical tools to easily drill-down into data to understand the impact of organizational changes on the workforce

One important aspect of process and analytics which was addressed in *Best Practices for Planning a Cybersecurity Workforce White Paper* is performing a supply and demand analysis. For the application of the CMM, it is important to note that cybersecurity demand can be segmented into three main work buckets: maintenance, attack, and defense. Some of these work categories are conducive to driver-based forecasting (e.g., maintenance) and some are not (e.g., attack and defense).

- *Maintenance* refers to work that involves the maintenance of systems, such as servers, and is demand data that organizations can use to predict the amount of work in the future because the volume of work is associated with the number of servers they have to operate and maintain
- *Attack Operations* refer to the work that cybersecurity professionals do to strike the enemy, and is demand data that is based on the organizations' authority. Therefore, workforce practitioners can potentially set their volume of work accordingly; however, the ability to predict future need may be limited
- *Defense Operations* refer to the work that cybersecurity professionals do to safeguard and protect U.S. networks and systems from attack. Unlike maintenance, defense workload is not conducive to quantified future estimates because of the unknown enemy threat and capabilities. In other words, cybersecurity defense workload cannot be measured in a standard way because establishing metrics and tracking work from a historical perspective will not be predictive of the evolving and changing future threats. Therefore, demand forecasting for the cybersecurity workforce is an exercise in prioritizing efforts and ensuring that there is adequate coverage across cybersecurity activities, and understanding the balance between strategic and tactical skill sets that might be needed.

The NICE Cybersecurity CMM takes these distinct characteristics regarding demand into account, and helps workforce practitioners think through the way in which they can segment types of demand work. The process and analytics segment is described by maturity level and related activities in Table 3.

[9] Risks may include issues such as lack of staff to recruit new professionals or a lack of funding to hire new staff. Organizations might also deem risks as having a large percentage of their population retirement eligible or the fact that they have no junior staff in specific areas of the organization.

Table 3. Process and Analytics Area

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Process	An organization has a limited workforce planning capability in the area of Process if they have evidence of the following: • Workforce planning efforts have only occurred at a sub-organization level • Results of these efforts have informed decisions for each sub-organization, which may or may not have been communicated up to the corporate level • Performance against these efforts have not been formally assessed	An organization has a progressing workforce planning capability in the area of Process if they have evidence of the following: • Workforce planning efforts have been conducted organization-wide for a specific assessment requirement or major change in mission or budget drill • Previous, org-wide efforts have been driven at the corporate level through data calls to the lines of business • Results of these efforts have informed point-in-time decisions regarding human capital programs or a strategic human capital planning effort • Performance against the efforts were not formally assessed	An organization has an optimized workforce planning capability in the area of Process if they have evidence of the following: • Established process for conducting organization-wide workforce planning tied to annual budget and business planning processes • Process is driven at the corporate level, but fully implemented within each line of business • Results of the process are utilized to drive changes in organization-wide human capital programs and investments • Performance against the process is assessed on an ongoing basis, and continuous improvements are made
Analytics	An organization has a limited workforce planning capability in the area of Analytics if they have evidence of the following: • Supply & demand data are only available through ad hoc data calls • The data must be manually processed and manipulated for analysis and reporting purposes • Few analysis tools, models, and/or templates may exist but are insufficient to support consistent analysis	An organization has a progressing workforce planning capability in the area of Analytics if they have evidence of the following: • Supply & demand data are available from various data sources, to include data calls, but may not be complete or up-to-date • This data requires compilation, manual processing, and quality reviews for use in analysis and reporting • Various analysis tools, models, and/or templates may exist for supply and/or demand data, but are insufficient to support full workforce planning analysis	An organization has an optimized workforce planning capability in the area of Analytics if they have evidence of the following: • Complete supply & demand data is available from authoritative data sources • This data can be easily accessed and manipulated for analysis and reporting purposes with minimal manual processing • Multiple analysis tools, models, and/or templates exist for both supply & demand data, and are sufficient to support full workforce planning analysis

Integrated Governance

Integrated governance represents those activities associated with establishing governance structures, developing and providing guidance, and driving decision-making. It is the building block to an organization's overall workforce planning strategy and vision. The integrated

governance enables an organization, through assignments of responsibility, promotion of integration, and issuing of planning guidance, to implement the tactics necessary to reach an overall mature workforce planning capability.

For the purpose of this paper, *governance structure* is explained by the definition established in The *Best Practices for planning a Cybersecurity Workforce White Paper*, where governance is defined as the set of processes, policies, and procedures affecting the way people direct, administer or control an organization. Governance also includes the relationships among the many players involved such as stakeholders and the organization's strategic goals.[10]

Cybersecurity managers are on the forefront of understanding the requirements and what drives the cyber workforce and workload, so it is essential that this group of individuals has input and plays a role within an organization's approach to integrated governance.

Table 4 provides the integrated governance activities across the three maturity levels.

[10] For more detail on the linkages between the Integrated Governance and the Strategy component established in the Best Practices for Planning a Cybersecurity Workforce White Paper, see Appendix C.

Table 4. Integrated Governance Area

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Integrated Governance	An organization with a limited workforce planning capability has evidence of Integrated Governance: • No established governance structure at the corporate level • Limited or ad hoc corporate level workforce planning guidance that considers workforce planning implications based on changes in budget, mission priorities, and/or policy changes • Decentralized decision-making at the sub-organization level	An organization with a progressing workforce planning capability has evidence of Integrated Governance: • Established governance structure that exists in either an Human Capital office, CFO Office, or Business Planning office, reaching to other entities as stakeholders in the process • Documented workforce planning guidance when major change in mission, program, or policy occurs to communicate workforce planning priorities and/or constraints related to the specific change • Workforce planning guidance is utilized to support planning process for a point-in-time corporate decision • Results drive short term decision on point-in-time corporate decision	An organization with an optimized workforce planning capability has evidence of Integrated Governance: • Established corporate level governance structure comprised of an integrated leadership group from CFO, Human Capital, and Lines of Business • Documented workforce planning guidance that incorporates implications of strategic, environmental, and policy issues to formulate workforce planning priorities and/or constraints • workforce planning Guidance is utilized to drive a regular (e.g. annual), organization-wide workforce planning process • Results drive both short term and long term decision making at a corporate level

Skilled Practitioners and Enabling Technology

Skilled Practitioners represents the activities associated with establishing a professional cadre of workforce planners within an organization. ***Enabling Technology*** represents the activities associated with the accessibility and use of data systems.

The skilled practitioners section of this area describes existence and characteristics of the workforce planning cadre. It is important to note that the workforce planning cadre does not have to be strictly dedicated to workforce planning with no other duties or responsibilities, but rather that the action of workforce planning can be a designated role within an organization, fulfilled by individuals that have other duties and responsibilities that are unrelated.

For the purpose of this paper, *skilled practitioners* are explained by the definition established for "people" in *The Best Practices for Planning a Cybersecurity Workforce White Paper*[11]. *People* focuses on a healthy, appropriately skilled and aligned workforce that is supported by effective human capital processes and practices.

The enabling technology section of this area focuses on the quality and integration of workforce planning systems and links to the technology section of the infrastructure component established in the *Best Practices for Planning a Cybersecurity Workforce White Paper*. *Technology* refers to

[11] Ibid.

the building and maintaining of systems, tools, and capabilities to support workforce planning specialists who integrate and execute key workforce planning activities. An important aspect of the cybersecurity workforce is that it is highly technical, requiring extensive education and/or experience. Thus, it takes a long time to grow an accomplished and experienced cybersecurity workforce. Similarly, it takes time for those planning for the workforce (i.e., workforce practitioners) to develop a baseline understanding of the work cybersecurity professionals perform. The levels of maturity designated within the CMM accounts for this extended period of time and levels of knowledge.

Table 5 lists the NICE Cybersecurity Workforce Planning CMM for skilled practitioners and enabling technology in the three maturity levels.

Table 5. Skilled Practitioners and Enabling Technology Area

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Skilled Practitioners	An organization has a limited workforce planning capability in the area of Skilled Practitioners if they have evidence of the following: • There are few personnel designated to support workforce planning-related efforts as they occur in the organization • This staff exists only at the corporate level, or in some cases, only at the sub-organization level • This staff does not actively share knowledge with others	An organization has a progressing workforce planning capability in the area of Skilled Practitioners if they have evidence of the following: • There are a number of personnel designated to support workforce planning-related efforts as they occur the organization • This staff exists either at the corporate level and/or sub-organization level • This cadre share knowledge on an ad hoc basis as needed to support the efforts as they occur	An organization has an optimized workforce planning capability in the area of Skilled Practitioners if they have evidence of the following: • Established cadre of skilled practitioners trained in the organization's workforce planning process and associated analytics • This cadre exists at both the corporate level and throughout the sub-organizations in sufficient numbers to support all aspects of the workforce planning process • This cadre regularly shares knowledge to promote skill building and continuous process improvement
Enabling Technology	An organization has a limited workforce planning capability in the area of Enabling Technology if they have evidence of the following: • Existing data systems and tools must be accessed by a limited pool of authorized users to pull down data and reports needed for workforce planning analysis • There is not centralization of existing tools, models, or templates for the organization's workforce planning community to access • Data that does exist must be integrated manually	An organization has a progressing workforce planning capability in the area of Enabling Technology if they have evidence of the following: • Some data systems, tools, and models can be used by the broader workforce planning community, but several of these systems and tools still require specific technical skill to access and manipulate information • Analysis tools, models, and templates may be accessed on a shared folder or share point site, but data systems must still be accessed separately • Data from various systems and models must be integrated manually without benefit of automation	An organization has an optimized workforce planning capability in the area of Enabling Technology if they have evidence of the following: • Authoritative data systems, analysis tools, and models are built in modern, stable applications that can be used by a wide range of practitioners, regardless of technical skill • A web portal or comparable capability exists to access the full range of data systems, analysis tools, and models used by the workforce planning community • There are automated ways to combine data from various systems to enable analysis and reduce manual processing

Achieving Maturity

Differing Maturity Goals

Organizations will have different goals when it comes to the maturation of the cybersecurity workforce planning capability and all organizations do not need to reach the optimizing state. Just as there are tradeoffs in determining what strategy to pursue, organizations may face tradeoffs and must evaluate opportunity costs when it comes to deciding in which maturity state they want to eventually end. This decision should take into account many different variables. Leaders need to assess the impacts of: allocation of resources, implementation, timing, and return on their investments. Therefore, organizations should view their maturity rankings less as a grade or judgment and more as an indication of resources spent on workforce planning. Having a "limited" maturity level, which means the organization is at the beginning of its capability development without established processes, lacking clear guidance and having little in terms of data and analysis methods, does not equate to "bad" workforce planning; rather, it indicates that the organization has not dedicated resources to partially or fully develop that aspect of the maturity model, and that there are extenuating circumstances for the limited maturity outcome.

> *Not every organization with a cybersecurity workforce needs to reach an optimized state across the entire CMM. The purpose of the CMM is to aid organizational leaders to evaluate trade-offs and make decisions on how best to progress its workforce planning capability based on the organization's current reality.*

For example, an organization that does not have many cybersecurity professionals - (Federal Agency A) - does not necessarily need a sophisticated web portal to track and maintain their cybersecurity workforce. This organization might find it is easier to maintain a simple database to track the handful of personnel they have aligned to cybersecurity, and thus realize that their resources are better used for other opportunities. Therefore, this organization may choose to never reach the optimizing maturity level as it relates to enabling technology.

Similarly, an organization that already has a robust workforce planning capability for its mission critical occupations/positions might not deem it necessary to develop an entirely separate process to track, manage, and analyze the cybersecurity workforce. Instead, this organization can simply include the cybersecurity workforce as part of the already tracked populations, ensuring that workforce planners utilize cybersecurity data for planning and decision making purposes. As a result, this organization may not aspire to an optimized maturity in process and analytics as defined by the CMM because it can meet its planning needs via another avenue.

Assessing Current Capability

Assessing an organization against the CMM is a three-part process, as described in the Figure below:

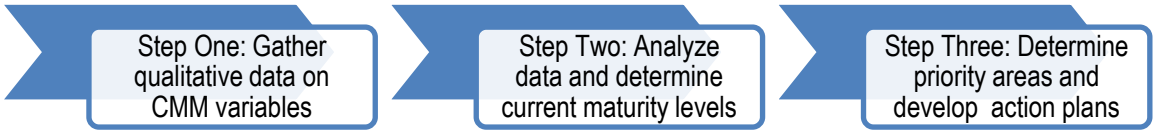


Figure 4. Assessment Process

Step One: Gather Data

The starting point for any organization to determine its cybersecurity workforce planning capability is for its leaders to assess the organization against the CMM. To do this, leaders must gather

qualitative data from across their organization which is specifically focused on the CMM and the variables within the areas. This data-gathering exercise will be qualitative and could be done through focus group interviews.

- For the *process and analytics* area, an organization needs to collect data on: the existence, integration, and robustness of the workforce planning process; the existence of feedback mechanisms; the availability and quality of supply and demand data; and workforce planning tools
- To ascertain the maturity for *integrated governance*, an organization needs to collect data on the existence of a governance structure, guidance, and evidence of linkages between workforce planning guidance and decision making
- Finally, for the *skilled practitioners and enabling technology* area, an organization needs to collect data on the existence and robustness of a workforce planning staff; evidence of knowledge sharing tools; and the accessibility and quality of workforce planning data systems

Table 6 shows the CMM area with corresponding data points.

Table 6. CMM Data Points

Capability Criteria	Data Points
Process and Analytics	• Workforce planning process at organization/Sub-organization level • Feedback mechanisms • Supply and Demand Data
Integrated Governance	• Governance structure • Workforce planning guidance • Organizational/Sub-organizational decision making
Skilled Practitioners and Enabling Technology	• Workforce planning staff • Knowledge sharing tools • Workforce planning data systems

Step Two: Analyze Data and Determine Current Maturity

Once the data has been collected, the organization will analyze it through the lens of the CMM maturity levels in order to determine the current level of maturity. Because the CMM is a management tool, the evaluation of maturity is a qualitative decision, supported by evidence of activities and infrastructure at an organization. As previously stated, the CMM is not a scorecard or report card, but rather an evaluation on where an organization falls as it relates to the cybersecurity workforce planning capability.

It is important to note that an organization can have various levels of maturity across the CMM; an organization can be limited in skilled practitioners and enabling technology, but progressing in integrated governance and process and analytics.

Another important detail is that general practice when using a CMM is to default to the lowest maturity level for the organization – or the lowest common denominator in ranking. For example, if three of five sub-organizations have workforce planning cadres and the other two do not; the organization would still default to an overall maturity rating of limited for “skilled practitioners and enabling technology. Ultimately, this ranking is decided on by the leaders of the organization.

For example, an organization might discover that there are pockets of workforce planning happening at the sub-organizational level through established processes and that some supply

and demand data feeds those processes. However, the supply and demand data is only available to a select group of individuals, mostly through compilation of internal databases, so there is some question around its quality. Additionally, the data is not housed in a system, but rather emailed to those individuals who might need it. Finally, headquarters does not base decisions on any sub-organizational analysis and does not perform its own workforce planning. As a result, from these data points, the organization would fall within the "limited" maturity level for process and analytics.

Table 7 illustrates an example of the evidence an organization might document as a result of a data call with the corresponding maturity levels using Harvey Balls (with an empty ball being least mature and a filled ball being most mature).

Table 7. Example Current Maturity Rating

Capability Criteria	Evidence	Maturity Rating
Process and Analytics	• Workforce planning processes at both the HQ and at Sub-organization level • HQ issued a data call to sub-organizations on cybersecurity workforce before making a strategic • Supply and Demand Data exist and is used, but the process is arduous and there is some questions about its accuracy due to lag time	◑
Integrated Governance	• Workforce planners sit in the Human Capital offices at HQ and sub-organizational level • During a significant re-org, leadership put out guidance on how to manage and realign the cybersecurity workforce so that it would experience as little disruption as possible • HQ issued a data call to sub-organizations on cybersecurity workforce before making a strategic	◑
Skilled Practitioners and Enabling Technology	• Workforce planners sit in the Human Capital offices at HQ and sub-organizational level • Workforce planners receive training on some supply and demand analysis • There are no established communication channels between workforce planners; sharing information is not a common practice • Systems exist, but the process is cumbersome because WF planners have to weed through several systems and databases • WF planners manually update their data	◑

Step Three: Progressing in Maturity

By assessing current cybersecurity workforce planning capabilities against the CMM, organizations can determine their next step priorities to further their progression along the maturity model. As previously mentioned, it is important to note that there are tradeoffs and impacts associated with these decisions and that organizations must consider the full spectrum of consequences resulting from resource allocation. Known risks include:

- Applying resources to areas that are not fully established, which may result in inconsistent processes or methods
- Unreliable support and infrastructure to enable change, which may result in inconsistent implementation across the organization
- Lack of stakeholder engagement, which may result in uneven messaging of the overall initiatives

It is likely than an organization will have to prioritize its maturity progression because there are finite resources available. Organizations should use the following method for progression:

1. Determine prioritized capability criteria (e.g., integrated governance)
2. Choose variable within capability criteria (e.g., governance structure)

3. Determine available resources for progression (e.g., time, resources, people to implement)
4. Understand action that is needed to move organization from one maturity level to the next (e.g., to get from limited to progressing for governance structure, an organization must establish a governance structure at the corporate level)
5. Develop Action Plan to fulfill maturity criteria
6. Implement the Action Plan
7. Refine as needed

The CMM analysis is a repeatable process. Any time an organization has the resources or capability to make progress, they can employ the above outlined methodology. There is no timeline to how long an organization can remain at a specific maturity level, and it is possible for an organization to advance in more than one criterion at once. For example, an organization can build its capability in both the integrated governance and process and analytics areas during the same time period. The only limited factor is an organization's wherewithal.

Benefits of Achieving Cybersecurity Workforce Planning Maturity

As previously written in the "Making the Case" section of this paper, there are several benefits to achieving cybersecurity workforce planning maturity. Additionally, it was also stated that some organizations might choose to pursue a less than optimized maturity. Therefore, it is important to note that organizations can still realize benefits regardless of their maturity levels. In fact, depending on the level of maturity achieved, organizations will experience a wide variety of benefits as a result of taking some actions and furthering their capability development. Table 8 segments many of these benefits by CMM area.

Table 8. Benefits to Reaching Workforce Planning Maturity

Capability Criteria	Benefits to Achieving Maturity
Process	• Increased consistency in execution of organization-wide Cybersecurity workforce planning activities • Enhanced data-driven decision making and analysis around shaping, building, growing, and supporting Cybersecurity workforce • Better understanding of integration points and hand offs between HQ, sub-organizations, and stakeholders for cyber workforce planning
Analytics	• Enhanced confidence and credibility in HQ decisions from the field and cyber workforce planning guidance • Decreased response times to analysis requests and external reporting requirements, enabling timely decisions to modify/change cyber workforce policy as needed and proactively • Decline in redundancy of data calls and burden of analysis efforts at all levels of the organization
Integrated Governance	• Enhanced view of current and future cybersecurity workforce and cyber workload • Better informed, proactive and policy-driven decision making around where to place and how to grow, resource and allocate Cybersecurity professionals • Increased organizational alignment and pragmatic solution development between workforce, human capital, budget, and strategic planning
Skilled Practitioners	• Increased employment of workforce planning process and decision methodologies • Improved culture of collaboration and swift sharing o f best practice information • Creation of a career path and professionalization of workforce planning group
Enabling Technology	• Enhanced confidence and credibility in decisions and released workforce planning guidance • Decreased response times to analysis requests and external reporting requirements • Increased amount of workforce analysis performed at all levels within the organization

Conclusion

The cybersecurity community has taken several positive steps towards developing its workforce planning capability as a whole. This White Paper serves as the follow on step to the *Best Practices for Planning a Cybersecurity Workforce White Paper* which encouraged further dialogue between NICE and Federal, state, local, tribal and territorial governments, industry, and academia to develop workforce planning approaches for the cybersecurity field. The purpose of this White Paper was to present a cybersecurity-specific workforce planning CMM so that organizations can baseline and benchmark their capabilities.

With the understanding of the foundational components of workforce planning established in the *Best Practices for Planning a Cybersecurity Workforce White Paper* (i.e., ***strategy, process,*** and ***infrastructure***) and the insights gained through the definitions of ***process and analytics***, ***integrated governance,*** and ***skilled practitioners and enabling technology*** as they relate to capability development***,*** organizations can now move forward to assess their workforce planning maturity using the NICE CMM. By doing so, organizations will identify the necessary priorities to invest in further so that they are able to proactively plan for, manage, shape, and grow their cybersecurity workforce.

Appendix A. Best Practices for Planning a Cybersecurity Workforce Components

Component	PROCESS	STRATEGY	INFRASTRUCTURE
	Establishes an integrated and consistent means of diagnosing workforce needs and risks	*Provides a direct line of sight between business and workforce requirements*	*Supports execution of an effective and repeatable workforce planning process*
Elements	***MODEL:*** Defines a common workforce planning process that is integrated with other strategic, business and human capital planning processes ***DATA:*** Identifies robust, relevant, consistent and quality data for targeted evaluation and problem solving ***ANALYTICS:*** Relies on various modeling and analysis techniques to organize, visualize, and assess demand, supply and structure data, to identify risks and inform solutions	***SHARED VISION:*** Provides a long-term view of an organization's strategic direction & business objectives, aligned to the labor supply & demand needed to meet those objectives ***GOVERNANCE:*** Ensures accountable decision making and sustains the structures and processes that turn decisions into actions ***PERFORMANCE:*** Encourages continuous monitoring, assessment and prioritization of workforce planning activities to balance workload and workforce requirements	***PEOPLE:*** Focuses on a healthy, appropriately skilled and aligned workforce that is supported by effective human capital processes and practices ***COLLABORATION:*** Combines top-down leadership and bottoms-up participation to enable the organization to collaborate and manage organizational knowledge ***TECHNOLOGY:*** Builds & maintains systems, tools and capabilities to support workforce planning specialists who integrate and execute key workforce planning activities

Appendix B. Process Defined

The generally accepted steps for a workforce planning process are:

- ***Step One:*** The process begins with a thorough inventory of the organization's supply, or in other words, the current workforce, considering the skills, characteristics, positions, and other pertinent information specific to the organization. This inventory serves as a baseline for the current state of the organization's workforce.
- ***Step Two:*** A ***demand*** and ***supply data analysis*** is then conducted. A ***supply data analysis*** looks at the positions and skills sets of current workforce to determine "who" is doing the actual work, whereas a ***demand data analysis*** examines an organization's goals and strategic plans and determines what the workload is for the current workforce. Depending on the organization's need, it may be easier for one data analysis to be conducted prior to the other[12]; however, both analyses are necessary for an effective workforce planning process.
- ***Step Three:*** At this point an organization analyzes both sets of data to identify gaps in current supply and expected demand. A workforce planning ***gap analysis*** will observe what actions need to be taken for an organization's current workforce to reach the organization's future workload needs.
- ***Step Four:*** Once the analysis is completed, the organization will create an ***implementation plan*** detailing the steps that need to be taken to eliminate or mitigate any gaps in the workforce. These steps will address an organization's needs to properly plan for its workforce.

This process provides basic elements of workforce planning processes for any organization whether public or private.

The Public Sector approach is from the Federal Government Human Resources Office. The five-phase, demand analysis driven methodology is the most established workforce planning methodology among Federal government agencies.

Table B-1. Public Sector Best Practice Process Approach

Phase	DESCRIPTION
Phase 1	Assess the strategic plan and identify future goals to define the future view of the organization. This provides a basis for determining what workforce will be necessary to support the future vision.
Phase 2	Review and analyze qualitative and quantitative workforce metrics to understand current resources, possibly using workforce analytics tools to facilitate the process. Determine the future landscape of the organization, or the type and number of workers as well as the work that will need to be performed. Identify the gaps.
Phase 3	Develop an action plan to close the workforce gaps. Create strategies regarding organizational decisions to recruit, train, or otherwise manage the workforce gaps. Establish success measures to ensure the organization is achieving its goals along the way.
Phase 4	Implement the action plan and ensure resources are in place. Due to the level of transition and change, communication resources are especially critical.
Phase 5	Conduct assessments throughout to ensure accomplishment of the end goal, and to manage any changes in environment or the organization that will impact the workforce needs of the organization. The plan may need to be adjusted along the way due to emerging issues.

[12] Depending on the structure and history of the organization, one data gathering method may be preferred or fit with the data sets better than another. Organizations with a long history and defined structure may find it valuable to do a demand analysis prior to supply because they have good data on their current workforce structure. A younger, less structured organization may find it necessary to do a supply analysis first to fully capture what resources are available to the organization. Following that step, the younger organization can look at where their mission needs to go and can conduct a robust demand analysis. Even though both sets of data need to be reviewed, organizations have to understand where they are in terms of growth and what data analysis is most beneficial to conduct first.

The Private Sector approach is from a Private Professional Services Firm, and is a four-phase supply data driven methodology.

Table B-2. Private Sector Best Practice Process Approach

Phase	DESCRIPTION
Phase 1	Collect current workforce data from Human Resource Information Systems (HRIS) and other sources, such as surveys or assessment techniques, for baseline data on current workforce skill sets. Validate data with HR or managers.
Phase 2	Conduct an analysis of organization workload to understand work produced and performed. Statistical analysis and other tools may add in analysis. Determine the workforce capabilities needed to accomplish identified work.
Phase 3	Identify future demands for workforce needs, creating a clear, accurate picture of the future needs of the organization. Accomplish analysis using historical and current data to analyze trends, and/or using workforce analytics tools to model data or consider risk factors. Conduct a gap analysis on current and future supply/ demand of the organization. Identify workforce objectives and determine workforce development strategies.
Phase 4	Develop and implement an action plan with a detailed timeline and phased approach. Train a cadre of employees in the organization on workforce planning practices to monitor progress and impact of any changes within the environment or the organization. Define levels of ownership, structure and reporting, to ensure there are mechanisms for improvement and to provide feedback on execution.

Appendix C. Governance Structure Defined

A *governance structure* consists of the set of processes, policies, and procedures affecting the way people direct, administer or control an organization. Governance also includes the relationships among the many players involved such as stakeholders and the organization's strategic goals. It is generally accepted that successful workforce planning governance structures include:

1. ***Guidance materials*** for ongoing review of the workforce
2. An ***internal panel*** of leadership and HR representatives to review the workforce planning process, including, but not limited to, representation from:
    - Senior leaders
    - Financial and budgetary representatives
    - Human capital experts and CoPs
    - Cybersecurity managers
    - Risk and loss prevention specialists
3. A ***feedback mechanism*** to ensure timely course correction in the planning process

A governance board is imperative to any cybersecurity workforce planning approach, as the fast-changing needs of cybersecurity can be otherwise overlooked. By incorporating an internal panel of individuals into the strategy, cybersecurity needs may be more effectively incorporated into the fiscal and strategic plans of an organization. Manager interaction with senior leadership would allow current cyber environment activities to be integrated into planning, and feedback would allow for timely adjustments to highly technical forecasts of the cybersecurity workforce.

Appendix D. NICE CMM

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Process	An organization has a limited workforce planning capability in the area of Process if they have evidence of the following: • Workforce planning efforts have only occurred at a sub-organization level • Results of these efforts have informed decisions for each sub-organization, which may or may not have been communicated up to the corporate level • Performance against these efforts have not been formally assessed	An organization has a progressing workforce planning capability in the area of Process if they have evidence of the following: • Workforce planning efforts have been conducted organization-wide for a specific assessment requirement or major change in mission or budget drill • Previous, org-wide efforts have been driven at the corporate level through data calls to the lines of business • Results of these efforts have informed point-in-time decisions regarding human capital programs or a strategic human capital planning effort • Performance against the efforts were not formally assessed	An organization has an optimized workforce planning capability in the area of Process if they have evidence of the following: • Established process for conducting organization-wide workforce planning tied to annual budget and business planning processes • Process is driven at the corporate level, but fully implemented within each line of business • Results of the process are utilized to drive changes in organization-wide human capital programs and investments • Performance against the process is assessed on an ongoing basis, and continuous improvements are made

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Analytics	An organization has a limited workforce planning capability in the area of Analytics if they have evidence of the following: • Supply & demand data are only available through ad hoc data calls • The data must be manually processed and manipulated for analysis and reporting purposes • Few analysis tools, models, and/or templates may exist but are insufficient to support consistent analysis	An organization has a progressing workforce planning capability in the area of Analytics if they have evidence of the following: • Supply & demand data are available from various data sources, to include data calls, but may not be complete or up-to-date • This data requires compilation, manual processing, and quality reviews for use in analysis and reporting • Various analysis tools, models, and/or templates may exist for supply and/or demand data, but are insufficient to support full workforce planning analysis	An organization has an optimized workforce planning capability in the area of Analytics if they have evidence of the following: • Complete supply & demand data is available from authoritative data sources • This data can be easily accessed and manipulated for analysis and reporting purposes with minimal manual processing • Multiple analysis tools, models, and/or templates exist for both supply & demand data, and are sufficient to support full workforce planning analysis

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Integrated Governance	An organization with a limited workforce planning capability has evidence of Integrated Governance: • No established governance structure at the corporate level • Limited or ad hoc corporate level workforce planning guidance that considers workforce planning implications based on changes in budget, mission priorities, and/or policy changes • Decentralized decision-making at the sub-organization level	An organization with a progressing workforce planning capability has evidence of Integrated Governance: • Established governance structure that exists in either an Human Capital office, CFO Office, or Business Planning office, reaching to other entities as stakeholders in the process • Documented workforce planning guidance when major change in mission, program, or policy occurs to communicate workforce planning priorities and/or constraints related to the specific change • Workforce planning guidance is utilized to support planning process for a point-in-time corporate decision • Results drive short term decision on point-in-time corporate decision	An organization with an optimized workforce planning capability has evidence of Integrated Governance: • Established corporate level governance structure comprised of an integrated leadership group from CFO, Human Capital, and Lines of Business • Documented workforce planning guidance that incorporates implications of strategic, environmental, and policy issues to formulate workforce planning priorities and/or constraints • workforce planning Guidance is utilized to drive a regular (e.g. annual), organization-wide workforce planning process • Results drive both short term and long term decision making at a corporate level

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Skilled Practitioners	An organization has a limited workforce planning capability in the area of Skilled Practitioners if they have evidence of the following: • There are few personnel designated to support workforce planning-related efforts as they occur in the organization • This staff exists only at the corporate level, or in some cases, only at the sub-organization level • This staff does not actively share knowledge with others	An organization has a progressing workforce planning capability in the area of Skilled Practitioners if they have evidence of the following: • There are a number of personnel designated to support workforce planning-related efforts as they occur the organization • This staff exists either at the corporate level and/or sub-organization level • This cadre share knowledge on an ad hoc basis as needed to support the efforts as they occur	An organization has an optimized workforce planning capability in the area of Skilled Practitioners if they have evidence of the following: • Established cadre of skilled practitioners trained in the organization's workforce planning process and associated analytics • This cadre exists at both the corporate level and throughout the sub-organizations in sufficient numbers to support all aspects of the workforce planning process • This cadre regularly shares knowledge to promote skill building and continuous process improvement

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Enabling Technology	An organization has a limited workforce planning capability in the area of Enabling Technology if they have evidence of the following: • Existing data systems and tools must be accessed by a limited pool of authorized users to pull down data and reports needed for workforce planning analysis • There is not centralization of existing tools, models, or templates for the organization's workforce planning community to access • Data that does exist must be integrated manually	An organization has a progressing workforce planning capability in the area of Enabling Technology if they have evidence of the following: • Some data systems, tools, and models can be used by the broader workforce planning community, but several of these systems and tools still require specific technical skill to access and manipulate information • Analysis tools, models, and templates may be accessed on a shared folder or share point site, but data systems must still be accessed separately • Data from various systems and models must be integrated manually without benefit of automation	An organization has an optimized workforce planning capability in the area of Enabling Technology if they have evidence of the following: • Authoritative data systems, analysis tools, and models are built in modern, stable applications that can be used by a wide range of practitioners, regardless of technical skill • A web portal or comparable capability exists to access the full range of data systems, analysis tools, and models used by the workforce planning community • There are automated ways to combine data from various systems to enable analysis and reduce manual processing

Appendix E. Acronym List

Acronym	Definition
AOR	Area of Responsibility
CMM	Capability Maturity Model
CNCI	Comprehensive National Cybersecurity Initiative
HR	Human Resources
NICE	National Initiative For Cybersecurity Education
U.S.	United States

Homeland Security

Department of Homeland Security
Contact Information:

Robin “Montana” Williams
Chief, National Cybersecurity Education & Awareness Branch
Email: Robin.Williams@hq.dhs.gov
Phone: 703.235.5169