Homeland Security

Department of Homeland Security

Best Practices for Planning a Cybersecurity Workforce White Paper

Version 2.0

August 4, 2014

Executive Summary

The Nation's cybersecurity workforce is at the forefront of protecting critical infrastructure and computer networks from attack by foreign nations, criminal groups, hackers, and terrorist organizations. Organizations must have a clear understanding of their cybersecurity human capital skills and abilities as well as potential infrastructure needs to ensure protection against threats to information systems. Today, the cybersecurity community has evolved enough to define a National Cybersecurity Workforce Framework for understanding specialty areas of cybersecurity work and workforce needs. As a result, the field has reached a maturity level that enables organizations to inventory current capabilities. Next, as the nation seeks to build a skilled cybersecurity workforce, it will be necessary for organizations to mature further and begin forecasting future demand for the cybersecurity workforce.

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 of people with the right knowledge and skills. Towards those ends, Component 3 of NICE is focused on the cybersecurity Workforce Structure — specifically the role of workforce planning in developing the national cybersecurity workforce. By identifying best practice[1] elements of workforce planning across three components— *Process, Strategy, and Infrastructure* – and the unique attributes of the cybersecurity workforce, this paper serves as a starting point to encourage discussion around the best methods for cybersecurity workforce planning and ultimately identifying an approach to address significant cybersecurity workforce gaps nationwide.

Approach

As the demands of global business, computing, and society continue to revolve around information technology (IT), cybersecurity workload is increasing faster than cybersecurity professionals can meet the demand. Workforce planning is used to address demand issues and close the workforce gap in a systematic way. To effectively consider this systematic approach in addressing cybersecurity needs, NICE addressed four questions in this paper:

1. *Does cybersecurity need workforce planning?*
2. *What are the best workforce planning methodologies for forecasting cybersecurity needs within organizations?*
3. *What governance structures and feedback approaches do the best workforce planning methodologies use?*
4. *Does the cybersecurity field pose any unique characteristics or criteria which could impact the way workforce planning is conducted for this specific group of people?*

Through research, NICE confirmed that the need for cybersecurity specialists is growing exponentially and there are simply not enough professionals to meet the demand. Internally, organizations are not able to develop and train enough cybersecurity professionals to keep pace

1 A best practice is defined as an approach or technique that has consistently shown results superior to those achieved with other means. Best practices were based on publically available information accepted to be true based on source.

with current requirements. Moreover, the rapid evolution and dynamic nature of cybersecurity makes maintaining, and retaining a well-qualified cybersecurity workforce challenging.

Using best practices, accurate workforce planning can identify skills and proficiency gaps across all cybersecurity roles. To address the four questions posed, best practices were synthesized from over 70 Federal organizations, conducted interviews, workforce planning benchmarking studies, Federal reports, and workforce planning guides and organized across three best practices components— *Process*, *Strategy*, and *Infrastructure.*

The analysis identified that successful *cybersecurity* workforce planning methodologies will need to employ specific best practices of each of the components, including risk assessments, customizable analysis tools, close monitoring of changes in skill sets, and agility in making quick course correction. Risk assessments and gap analysis are critical—the fast-changing cybersecurity environment presents a need to identify changes quickly in skill sets and gaps in supply. These practices will allow organizations to understand the rapid fluctuation of cybersecurity workload and workforce will affect infrastructure, financial, and physical risks.

To mitigate risks around gaps, customizable analysis tools that link workforce planning tools directly to the Human Resource Information System would allow for easy drill-down into data to understand the impact of organizational changes on cybersecurity workload and better manage fluctuations in need. Maintaining relevant tools, which assist in the cybersecurity workforce planning effort, saves time and money when forecasts must be changed to meet evolving needs. Enabling technology was also found to be a key differentiator in terms of leading infrastructure practices.

Considering organizational structures, NICE found that a balanced and integrated workforce planning governance structure ensures that a workforce planning cycle stays flexible and continuously provides information to an organization about its workforce. For cybersecurity planning specifically, a top-down and bottom-up approach to governance is a critical component. The nature of the technology is changing so rapidly that the involvement of cyber managers, talent management staff, and senior leaders is necessary to maintain speed with the external changes. Manager interaction with senior leadership would allow current cyber environment activities to be integrated into planning and for timely adjustments to highly technical forecasts of the cybersecurity workforce.

Additionally, cybersecurity workforce planning will require a shared vision and performance management. A shared vision will provide a common language and taxonomy to define cybersecurity workload and workforce allowing agile response to emerging technology and new threats. Performance management is also key to evaluating cybersecurity professionals' demonstrable skills of specific technology-based specialties. The National Cybersecurity Framework, developed in 2011, would provide additional support to organizations in considering this critical aspect of cybersecurity workforce planning.

One of the most important aspects of workforce planning is identifying the workforce and workload requirements that impact the nature of the work performed. Workload and workforce requirements are the unique characteristics that make one profession different from another, and may change how workforce planning is executed for that workload or workforce. NICE found unique workload and workforce requirements specifically important to cybersecurity:

<u>Workload Requirements:</u>

- ***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

Coupled with workforce planning best practices, these requirements help identify workforce planning needs as they apply to cybersecurity.

Next Step Recommendations

This paper recommends a two-pronged approach to accomplish next steps. Organizations should in fact use workforce planning to identify cybersecurity skills, proficiency gaps, and workload. An approach should be defined which integrates best practices for workforce planning specific to cybersecurity with the seven categories of The National Cybersecurity Workforce Framework—providing a standardized and categorized way from which to build this approach. Organizations should then use a Capability Maturity Model to apply the elements of best practice workforce planning to analyze their cybersecurity requirements and maturity needs.

Table of Contents

Introduction

Cybersecurity is at the forefront of protecting critical infrastructure and computer networks from attack by foreign nations, criminal groups, hackers, and terrorist organizations. To combat these threats, our nation depends on robust, agile, and highly trained cybersecurity workforce. Building such a workforce requires that organizations have a clear understanding of their current cybersecurity human capital skills and abilities as well as potential infrastructure needs to ensure protection against threats to information systems. Planning for the future cybersecurity workforce is critical to the safety and security of the nation.

The National Initiative for Cybersecurity Education (NICE) initiative is led by the National Institute of Standards and Technology (NIST) and is comprised of over 20 Federal departments and agencies, including the Component 3 lead – Department of Homeland Security (DHS). The goal of NICE is to enhance the overall cybersecurity posture of the United States. Component 3, the Cybersecurity Workforce Structure Strategy, has been tasked with evaluating the merits of workforce planning methodologies for the cybersecurity field.

> *"Cybersecurity is the most important national security issue confronting the United States today." – Former Chairman of the Joint Chiefs of Staff Peter Pace*

NICE Component 3 aims to gain consensus around defining best practice[2] methodologies for workforce planning capabilities for cybersecurity based on leading practices across the Federal, state, local, tribal, and territorial governments, industry, and academia. This paper serves as a starting point to encourage discussion around the best methods for cybersecurity workforce planning and ultimately identifying an approach to address significant cybersecurity workforce gaps nationwide.

To evaluate the merits of workforce planning methodologies for the cybersecurity field, this paper analyzes best practices which may support organizations' cybersecurity workforce planning. It explores best practices of workforce planning across a variety of Federal, state, and private industry organizations known for successful workforce planning. These best practices are evaluated against the primary components of general workforce planning methods – Strategy, Process, and Infrastructure – and their related elements. Particular attention is paid to elements which may have greater impact on cybersecurity workforce planning. In addition, unique workload and workforce requirements – characteristics specific to a particular profession – of the cybersecurity field were also defined in order to recommend the best approach for workforce planning specific to the cybersecurity workforce.

Background

Over the last decade, cybersecurity has become a national and global security concern. Nearly every business, government, school, and household is dependent on information technology (IT) and therefore susceptible to cyber vulnerability or attack. With the positive aspects of access to IT, comes the inevitable negativity of a way to exploit the technology.

Cyber-attacks, data theft, and security breaches know no limits. Cyber theft affects everything from personally-identifiable information to national secrets. A Norton study calculates the cost of global cybercrime at $114 billion annually.[i] Based on the value surveyed victims placed on time

2 A best practice is defined as an approach or technique that has consistently shown results superior to those achieved with other means. Best practices were based on publically available information accepted to be true based on source.

lost as a result of cybercrime, these attacks cost an additional $274 billion. With 431 million adult victims globally last year alone, the annual financial and operational losses due to cybercrime and attack exceed $388 billion globally. This number represents more than the global black market in marijuana, cocaine and heroin combined.[ii]

> *"The Federal government will not be able to combat cybersecurity threats without a more coordinated, sustainable effort to increase cybersecurity expertise in the federal workforce." - Cyber In-Security*

Until now, it has not only been hard to keep up with the changing security demands of cyber threats, but it was also challenging to even define what constitutes cybersecurity. Consequently, the overall workforce planning process for cybersecurity professionals across the nation was insufficient, making it difficult to plan for the right people to protect mission critical information. Today however, the cybersecurity community has evolved enough to define a framework for understanding specialty areas of cybersecurity needs[iii]3. Furthermore, the field has reached a level of maturity enabling organizations to inventory current capabilities and forecast the future demand for the cybersecurity workforce.

With 80 percent of industry organizations having experienced a large-scale denial-of-service attack, and 85 percent suffering network infiltrations[iv], the need to define and plan for the cybersecurity workforce stands as one of the most pressing needs of organizations across the globe. A well-governed, integrated workforce planning approach, steeped in best practices from successful governments and businesses, and aligned to the specialty areas of cybersecurity will provide tangible improvements to organizations' ability to accurately plan and protect.

Issue

Cybersecurity workload is increasing and there is a lack of cybersecurity professionals to meet demand. Workforce planning is one potential solution to address real workforce gaps in cybersecurity. *Workforce planning* is a systematic way for organizations to determine future human capital requirements (demand), identify current human capital capabilities (supply), and design implement strategies to transition the current workforce to the desired future workforce.[v] Four questions must be addressed in validating this solution.

1. Does Cybersecurity need workforce planning?

In 2011, General Accountability Office (GAO) released the report: *Cybersecurity Human Capital*, highlighting the cybersecurity workforce health of eight Federal agencies. The report found that these Federal agencies had trouble determining the size of their cybersecurity workforce and defining common workforce roles and responsibilities[vi]. Previous to the GAO report, the *Cyber In-Security* report characterizes the Federal government's cybersecurity talent as "decentralized and fragmented, making an accurate portrayal of the cybersecurity workforce difficult."[vii] This inability to understand the cybersecurity workforce effectively puts additional strain on organizations already facing massive costs in defending IT systems.

While most established organizations do not understand what workforce they have, developing and maintaining a competent cybersecurity workforce needs little justification and is, in fact, a

3 The National Cybersecurity Workforce Framework, puts forth a working taxonomy and common lexicon that organizes cybersecurity into seven high-level categories, each comprising several specialty areas. It has been developed largely with input from the Federal Government and is currently being refined by the nation's cybersecurity stakeholders, including academia, professional, and non-profit organizations, and private industry. http://csrc.nist.gov/nice/framework/

central requirement for ensuring resilient operations.[viii] This point is made clearer by the financial toll cybercrime costs businesses every day. The cost of cybercrime increased by 56 percent over the past year, and costs can rise dramatically if attacks are not resolved quickly[ix]. This makes the need for the right cybersecurity professionals in the right place even more critical to organizations.

Moreover, the rapid changes and dynamic nature of cybersecurity makes keeping a well-qualified cybersecurity workforce a big management challenge. The dynamic environment of cybersecurity often creates a skills gap in ensuring cybersecurity professionals are able to combat threats. Workforce planning will support organizations by 1) systematically identifying cyber professionals, in standardized terms, to accurately account for the current workforce; 2) identifying and quantifying the workload and workforce requirements unique to the organization; and 3) analyzing the skills and talent needed to fill the gap in workforce. Effective workforce planning is designed in a repeatable and reliable fashion, highlighting risks and forecasting needs over time.

2. *What are the best workforce planning methodologies for forecasting cybersecurity needs within organizations?*

A *workforce planning methodology* is a comprehensive and repeatable process that organizations can build upon when engaging in workforce planning.[x] Accurate workforce planning, using best practices, is a proven best practice in identifying gaps of needed skill sets and proficiencies that can fill multiple types of cybersecurity roles. For the critical and specialized roles of cybersecurity, including an agile workforce needed for surge capacity during times of increased attack or vulnerability, effective workforce planning can forecast demand. Common among all leading best practices are three broad components of workforce planning: ***Process, Strategy, and Infrastructure***. These best practice components are further divided into nine leading practices of workforce planning. These leading practices were evaluated against the cybersecurity workforce to benchmark best practices for cybersecurity workforce planning.

3. *What governance structures and feedback approaches do the best workforce planning approaches use?*

Cybersecurity is changing so rapidly that organizations often fail to plan for the necessary workforce or they hire incorrect skills sets, impeding their ability to protect themselves from cyber-attacks. Likewise, poorly functioning feedback mechanisms fail to define future cybersecurity needs for workforce planning within organizations. Workforce planning specialists cannot forecast cybersecurity needs without comprehensive governance structures. Well-governed, integrated workforce planning provides tangible improvements to an organization's ability to accurately define needs and plan. A proper governance structure also ensures that a workforce planning cycle stays flexible and continuously provides information to the organization about its workforce. A trademark of a good workforce planning approach is its ability to adapt based on different available data and timing cycles. Governance structures in cybersecurity workforce planning will be necessary to set the priorities of planning cycles and enforce the proper procedures and information sharing, so that any organization can realize optimal results from the workforce planning process.

4. *Does the cybersecurity field pose any unique characteristics or criteria which could impact the way workforce planning is conducted for this specific group of people?*

A cybersecurity workforce must be agile and flexible to react to changing threats, and also to able to surge in support during times of threat or attack. Like law enforcement, cybersecurity threats change as the enemy develops new technology and capabilities, and organizations must forecast

demand to combat future threats. Also, similar to emergency preparedness, cybersecurity professionals need to be able to respond quickly and accurately to any situation at any given time. To provide the most accurate best practices for planning for a cybersecurity workforce, characteristics like these must be accounted for in the way organizations understand their current workforce and plan for their future needs.

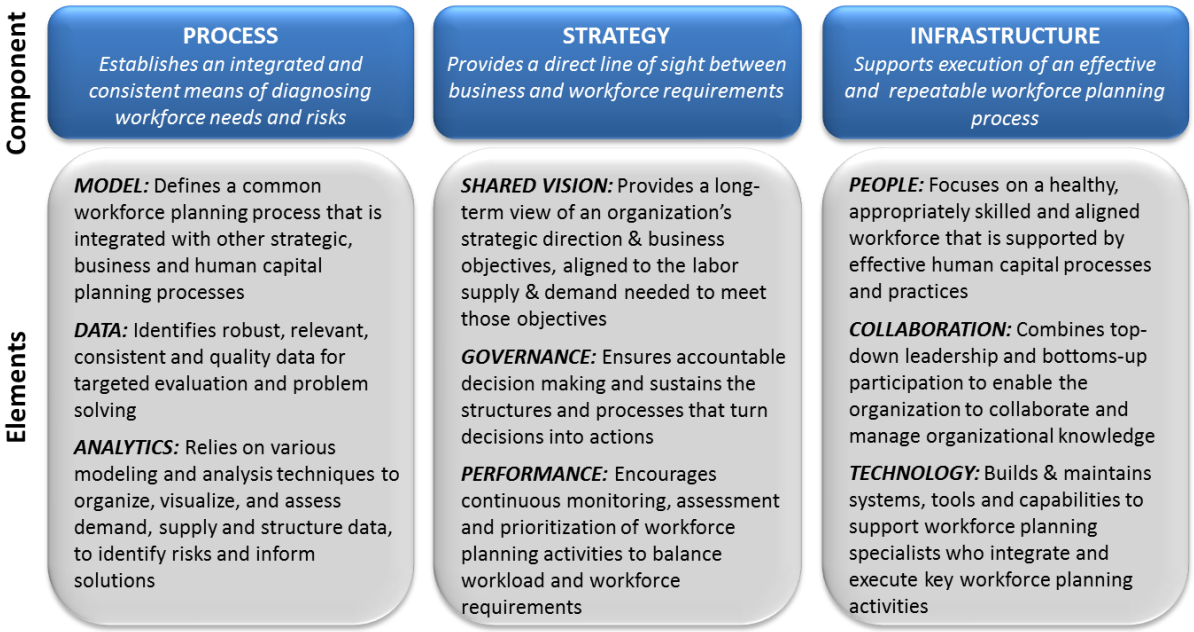
Approach

Effective workforce planning highlights areas of potential risk associated with aligning workforce to work. Applied correctly, workforce planning allows organizations to adjust resources to meet future workloads, patterns of work, and fundamental changes in how work is accomplished. In the case of forecasting the needs of the cybersecurity workforce, organizations must use a workforce planning approach that both fits the needs of the specific organization while accounting for unique characteristics of the cybersecurity profession.

Organizations conduct workforce planning in a unique way, and currently there is no recognized workforce planning approaches specifically for cybersecurity. Therefore, identifying best practice elements of workforce planning across organizations – specifically, the private and public sector – was selected as the approach for evaluating the merits of workforce planning for the cybersecurity field. The best practices below were gathered from various Federal organizations, interviews, workforce planning benchmarking studies (including the Partnership for Public Service[xi], AQPC[xii], and the Pew Center on the States[xiii]), GAO reports[xiv], and workforce planning guides, and organized into three broad components described in Figure 1 below. [4]

4 This research was complemented by over 10 years of Booz Allen Hamilton's workforce planning work with over 70 Federal organizations, state governments, and industry organizations, including in-depth capability building for the Department of Veterans Affairs.

Figure 1: Workforce Planning Best Practices by Component



Each of these components and corresponding elements of best practice workforce planning will be addressed through different analysis approaches.

In identifying comparative best practices for evaluating the merits of workforce planning for the cybersecurity field, organizations were surveyed from a variety of industry and government sectors and chosen based on reputation within the field and established workforce planning approaches. These organizations (Figure 2 below) exhibit components of good workforce planning and include protocols for addressing the workforce.

Figure 2: Organizations Exhibiting Components of Good Workforce Planning

Federal Government	State Government	Private Industry
► Defense Intelligence Agency ► Federal Aviation Administration ► National Aeronautics and Space Administration ► National Security Agency ► Office of Personnel Management ► United States Army ► UN Regulatory Commission	► Commonwealth of Virginia ► State of Carolina ► State of Georgia ► State of Indiana ► State of South Carolina ► State of Utah	► Boeing ► Booz Allen Hamilton ► Hewlett-Packard ► Human Capital Management Institute ► Qantas Airways Limited ► Starbucks Coffee ► The International Public Management Association for Human Resources

Best Practices in Workforce Planning Process

The evaluation of the ***Process*** component includes an in-depth analysis of each step of the workforce planning process through comparison of two different workforce planning methodologies. In both the public and private sectors, workforce planning has three commonly accepted process elements – model, data, and analytics. Together, these elements allow an organization to better understand the state of its workforce and address needs to properly plan for its workforce. Before examining these elements, it is important to understand the general workforce planning process.

The workforce planning process is commonly applied as a four-step activity. The generally accepted steps of the four-step workforce planning process are:

- ***Step One***: The process begins with a thorough inventory of the organization's supply, or its 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[5]; 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 determines what actions need to be taken for an organization's current workforce to reach the organization's future workload needs
- ***Step Four:*** Once the gap analysis is completed, the organization creates an implementation plan detailing the steps that need to be taken to eliminate or mitigate any gaps in the workforce. These steps 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. As such, these steps were used to set the criteria for evaluating best practice workforce planning processes, from both the public and private sector, in application of cybersecurity workforce planning. To gain a comprehensive look at workforce planning across the nation, one best practice workforce planning process was chosen from each the public and private sectors – specifically, a major Federal Government Human Resources Office and a private professional services firm – and is discussed in more detail in the next section.

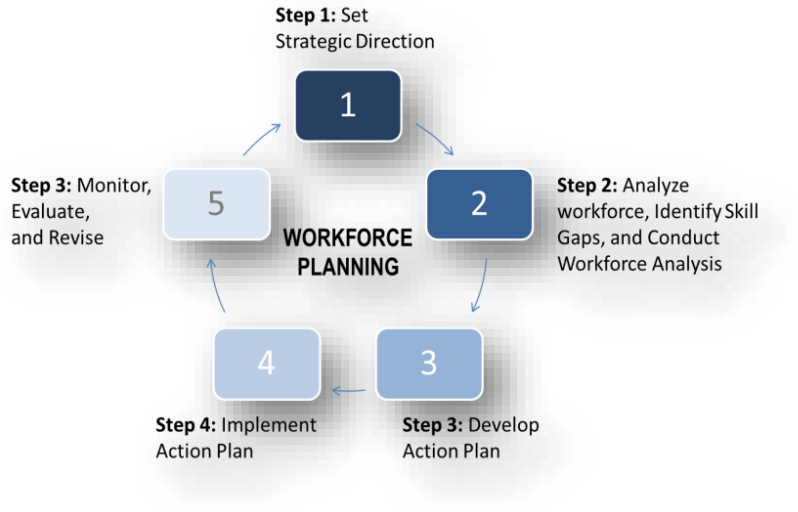
Overview of Workforce Planning Process Methodologies

This section delves into the representative workforce planning processes from both the public and private sector. For application in this analysis, processes will be referred to as methodologies. The section includes a visual depiction of the process and summary description.

The Public Sector approach (Figure 3) is from the Federal Government's Human Resources Office. The five-phase, demand-analysis driven methodology is the most established workforce planning methodology among Federal government agencies.

5 Depending on the structure and history of the organization, one data gathering method may be preferred or fit with the data sets better than the other. 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.

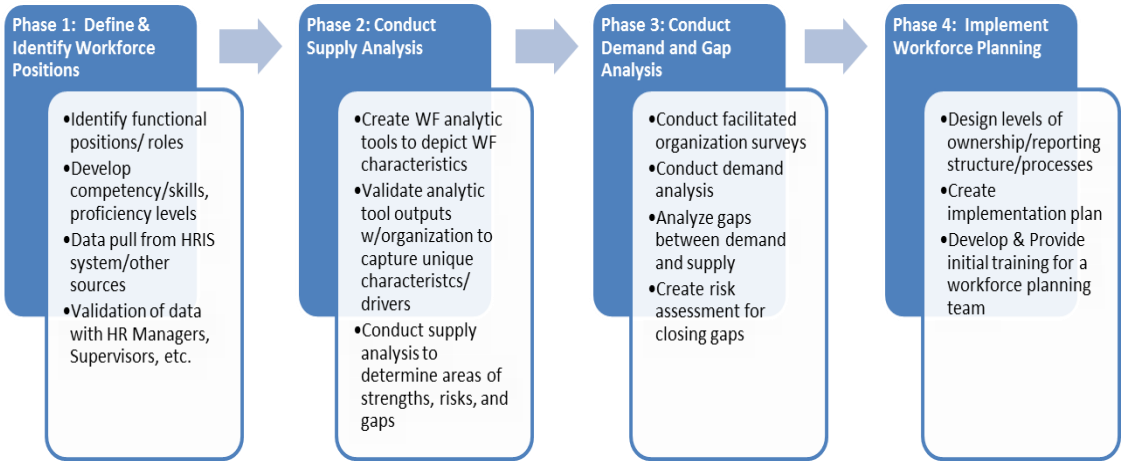
Figure 3: Federal Government's Human Resource Office- Workforce Planning Methodology



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.

Alternatively, the Private Sector approach of the Private Professional Services Firm presents a supply data driven methodology. This approach provides four phases with equal emphasis on each of the elements of the workforce planning processes.

Figure 4: Private Human Capital Consulting Firm - Workforce Planning Methodology



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 Human Resources (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.

Process Analysis – Workforce Planning Model, Data, and Analytics

To evaluate the merits of these best practice workforce planning methodologies for the cybersecurity field, the public and private methodologies were analyzed against the standard ***Process*** elements of workforce planning – model, data, and analytics – as well as additional supporting characteristics of these elements unique to each methodology. Both methodologies are data driven, relying on active participation by the implementing organization, and offering essential steps for developing the organization's workforce. Each methodology also addresses the main elements of a strong workforce planning process – model, data, and analytics. However, each focuses on varying supporting characteristics, applying the process elements in different order. This section addresses these similarities and differences, and the unique applications to the cybersecurity field.

Table 1 compares the major characteristics of each workforce planning process by related element:

Table 1: Characteristic Comparison of Workforce Planning Process Elements

		Public Sector Methodology		Private Sector Methodology	
Elements	**Characteristic**				
Data	**Supply Data Collection**	Yes	Phase 2	Yes	Phase 1, Phase 2
	Demand Data Collection	Yes	Phase 1	Yes	Phase 3
Analytics	**Gap Analysis**	Yes	Phase 3	Yes	Phase 3
Model	**Implementation Plan for closing Gaps**	Yes	Phase 3, Phase 4	Yes	Phase 4
	Supporting Characteristics				
Model	**Success Measurement**	Yes	Phase 3, Phase 5	Yes	Phase 4 (through consultation with implementation plan)
	Communications Planning	Yes	Phase 4	No	
Analytics	**Risk Assessment**	No		Yes	Phase 3
	Planning assessment and development tools	No		Yes	Phase 3

Regarding the *Data* element, there is some variation in order of approach. As Table 1 shows, while both methodologies include supply and demand data collection, each collects the data at different stages. The public sector methodology relies heavily on empirical data gained through analyzing the organization's mission, vision, and strategic goals to determine near-future workforce demand. The private sector methodology relies heavily on data collection using human resources databases and surveys, producing supply data about workforce roles and positions.

One cause for the difference in the decision to assess supply data or demand data first is likely organization type. Supply data is often easily accessible for Federal agencies, making demand analysis more valuable and harder to accomplish for these entities. On the other hand, supply data analysis may work best for private industry for similar reasons – market trends, historical data, strategic documents, and profit often provide greater accessibility to current data. In application to cybersecurity, the type of data with the greatest level of accessibility may be an important element in selecting the most appropriate model – either for the field or for an individual organization.

Regardless of the order in which the supply and demand data is evaluated, both methodologies follow with a gap analysis to show any shortage of resources and assess trends within the organization. Trends can include lack of a particular type of education, deficiency in staffing numbers, or missing skill sets. While similar in the *Analytics* element up to this point, the methodologies diverge on the whether to perform a risk assessment.

The private sector methodology calls for an assessment to examine potential risks to an organization's workforce development process and to consider mitigation solutions. 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. The public sector methodology never explicitly calls for a risk assessment; however, "Phase 5" does discuss continued monitoring of the workforce analysis to manage any changes that could impact the organization's workforce needs. The predominance of the risk assessment characteristic for each methodology may be linked to sector's ability to accept a certain amount of risk – a factor for consideration when applying cybersecurity requirements to workforce planning.

Risk assessments also help prioritize an organization's mitigation strategy because resources are finite. The risk assessment identifies the most pressing issues and helps focus action plans and solution sets.

The methods also diverge on the *Analytics* element in regards to the use of customized tools. The private sector methodology offers an analytics capabilities element which is planning for a technical field like cybersecurity. For example, Starbucks Coffee links their workforce planning tool directly to their HRIS to more easily drill-down into data to understand the impact of organizational changes on the workforce. The dynamic nature and complexity of cybersecurity may necessitate customizable analysis tools to make workforce determinations and maintain workforce planning.

Once the gap analysis is completed, both processes call for a sustainable *model element* – or an implementation or "action" plan to close the gaps addressed, suggesting a phased and detailed approach to execution. Each methodology considers whether training would benefit workforce development or if resources should be hired from outside the organization as well as the introduction of continuous monitoring and feedback opportunities – or *success measurements*. However, a unique supporting characteristic of the public sector methodology is a focus on communication. *Communication* is a pivotal aspect of executing a workforce planning action plan and supports shared understanding within the organization on expectations for managing the workforce. Focusing on communication and shared understanding is important when planning for a newer workforce like cybersecurity. It is also important to note that the implementation plan outlines the integration between business processes. Most likely, human capital specialist will work side-by-side with the workforce planning specialists to devise action plans to mitigate the risk – they are the tactical arm of the strategy that is identified by the workforce planning process.

Through analysis of these two best practice methodologies, it is evident that understanding the organizational type and the available data is critical to selecting the appropriate process for forecasting the cybersecurity workforce. Likewise, a risk assessment and gap analysis is critical to completing an accurate workforce assessment. Beyond that, the addition of a communications plan is useful for establishing a shared understanding across the organization for managing expectations and transitioning to a more robust cybersecurity workforce. Lastly, continuous monitoring and feedback is critical to the success of workforce planning for the fast changing cybersecurity environment.

Best Practices in Workforce Planning Strategy

In addition to establishing best practice-driven workforce planning processes, best practices from a strategy perspective inform organizations and optimize the forecasting ability for the cybersecurity field. The strategy best practices focus on provides a direct connection between organizations and their workforce requirements. Strategy-leading best practices include a shared vision, supported by strong governance, linked to performance outcomes. As mentioned above, these elements impact the workforce planning process as well as guide the ongoing efforts of building and maintaining a healthy workforce. The leading practices across these elements can easily be translated into application in a cybersecurity workforce planning environment.

Best Practices in Shared Vision and Performance Elements

A successful organization has a ***shared vision*** helping to define its purpose and values and orient itself towards external stakeholders. Likewise, successful workforce planning has to share in a vision that aims to build a workforce that allows organizations to achieve their goals at peak

performance – which includes continuous monitoring, assessment, prioritization of workforce planning activities, and balance workload and workforce requirements.

Shared vision and performance management are especially important in considering workforce planning approaches for cybersecurity. The 2011 GAO report, *Cybersecurity Human Capital,* calls for a more deliberate focus on workforce planning of cybersecurity in the Federal government and specifically recommends a comprehensive review of an agency's strategic plan to meet short- and long-term goals[xv]. Additionally, the report suggests involvement of top management, employees, and other stakeholders in development, communication, and implementation. The need to plan for current and future cybersecurity personnel has hit a critical point and incorporating best practices that improve this planning are imperative to success. As the list of best practices by the Strategy element(s) below indicates, a number of public and private sector cyber entities have already taken steps to meet these elements.

- The Defense Intelligence Agency used workforce planning to develop a framework for identifying workforce priorities to create a shared vision as they began rapid growth in specialized areas
- Qantas maintains quarterly updates for all workforce need forecasts, including five-year plans, to improve workforce planning performance
- The US Army predicted seven year forecast needs with their workforce planning system and developed a program to create future mid-level managers to meet those needs
- The State of Georgia uses its workforce planning system for assessing performance and quickly identifying skill sets where gaps are present to plan accordingly
- The Commonwealth of Virginia developed a workforce planning solution to assist in meeting the state's need to work better and spend less, including a thorough performance management system which enables transparency and information sharing

Each of these best practices was analyzed for application in a cybersecurity setting. A shared vision for cybersecurity workforce planning provides a common language and taxonomy to define cybersecurity workforce needs and quarterly adjustments allow the cybersecurity profession to be highly agile in responding to emerging technology and new threats. In many cases, the cybersecurity needs of an organization are so demanding that establishing mid-level managers in place for future cyber team build-out will be critical to growth success. The fast-changing cybersecurity environment presents a need to identify changes in skill sets as well as gaps in supply quickly. Performance management is key to evaluating not only the knowledge of cybersecurity workforce, but also the demonstrable skills of specific technology-based specialties.

Best Practices in Governance Structures

To maintain the workforce planning capabilities of an organization, an authority should be directed with monitoring and calibrating the process. This is the third element of the ***Strategy*** component of workforce planning. 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[xvi]. 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 Communities of Practice (CoPs)
- Cybersecurity managers
- Risk and loss prevention specialists

3. A ***feedback mechanism*** to ensure timely course correction in the planning process

Samples of best practices were chosen to provide comprehensive look at workforce planning governance structures. Each strategy approach to governance has been defined as a best practice and is discussed in more detail below:

- The National Security Agency (NSA) developed a Workforce Planning Counsel comprised of human capital representatives, senior leadership, finance department members, and managers to develop and maintain the workforce planning approach and outcomes for each forecast. Its feedback process is also an integral part of workforce planning improvement
- The Federal Aviation Administration (FAA) established a Human Capital Planning Council to serve as an internal COP for workforce planning and to provide a place to share best practices and disseminate guidance. The Agency designed a system of accountability to hold managers and human resource officers responsible for efficient and effective management of their workforce planning, including requiring executives to sign workforce planning documents for the workforces under their purview
- The State of Indiana created a "Workforce Planning Committee" consisting of representatives from the larger state agencies, as well as the Office of Management and Budget and the State Personnel Department. The committee collects and analyzes workforce data that focuses on hiring, turnover, and impending retirements, and assist agencies in developing formal workforce plans that address their specific needs

Each of these organizational structures possesses key components of governance. The FAA created guidance materials for how their governance structure operates in addition to their panel for discussing governance operations. The NSA example represents the need for an established feedback mechanism to review the workforce planning process. The State of Indiana example represents an established governance board analyzing the holistic workforce needs across the state to support all organizations. These best practices can be applied directly to the nuances of the cybersecurity workforce.

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 allows current cyber environment activities to be integrated into planning, and feedback allows for timely adjustments to highly technical forecasts of the cybersecurity workforce.

Best Practices in Workforce Planning Infrastructure

In addition to an integrated ***Strategy*** component to manage the workforce planning process, a well maintained and organized ***Infrastructure*** component supports ongoing collaboration across people and technology. The ***Infrastructure*** component focuses on supporting execution and effectiveness of a repeatable workforce planning process. Across all sectors, workforce planning

is understood to have three critical infrastructure elements – *people, collaboration, and technology*. Together these elements focus on health and skills of the workforce, collaborative management, and optimal tools and capabilities needed to plan for a successful organization.

Best Practices in People, Collaboration, and Technology

A successful workforce planning approach is influenced by how its parts interact. The people of the organization impact how it is structured based on their skills and abilities, and the way in which they collaborate with one another affects workforce planning. Additionally, technology, or the lack thereof, can help achieve the most accurate forecasts or cause impediments to workforce planning functions.

The examples listed below include leading practices in workforce planning infrastructure, such as staff commitment, customized monitoring, and collaboration among employees on managing the workforce structure.

- Hewlett-Packard developed a workforce planning Center of Excellence which requires only a small concentrated staff of highly skilled employees to serve as a strategic partner for managers to improve their workforce planning processes. Combining a highly-skilled human capital staff in close conjunction with the managers allows for better understanding of the critical and fast-changing requirements for future cybersecurity workforce structure
- The State of South Carolina designates a "workforce champion" within each agency, responsible for directing and encouraging agency activities among its employees with regard to workforce planning
- NASA's Workforce Planning Community of Practice, led by the Workforce Strategy Division of the Office of Human Capital Management, established an enterprise-wide system for workforce planning and developed key principles to monitor the Agency's approach to workforce planning. Participants included both agency and Center representatives to balance agency-wide needs and to clarify roles and responsibilities
- The FAA encourages collaboration among top management, employees, and other stakeholders in developing, communicating, and implementing a community of practice as a focal point for sharing best practices and disseminating guidance
- The State of Utah's Department of Human Resource Management's Strategic Data Management Initiative analyzes demographic data, provides HR data and analysis, and develops performance metrics for agencies. This is done in collaboration with the governor's "balanced scorecard initiative," a management system developed to assist agencies in clarifying their vision and strategy and translating them into action

Driving the focus on the people element and collaborating from a top-down and bottom-up approach is critical to cybersecurity planning. The nature of the technology is changing so rapidly that involving project managers, talent management staff, and senior leaders allows for immediate course correction in workforce planning helps keep pace with the external changes. Likewise, enabling technology was often shown as a key differentiator in terms of infrastructure related to leading practices. Maintaining relevant tools, which assist in the workforce planning effort, saves time and money when forecasts must be changed to meet evolving needs.

Cybersecurity Requirements

Understanding the requirements that make the job of cybersecurity unique is one of the most important aspects of cybersecurity workforce planning. Understanding these requirements will

help organizations achieve accurate plans and set themselves apart in this highly competitive marketplace. There are a number of workload requirements that drive the nature of the work and the work environment. Likewise, there are a number of workforce requirements that result from that unique environment. These varied and diverse requirements drive the needs of an organization in relation to its cybersecurity workload and workforce.

Cybersecurity requirements have been previously characterized through a number of Federal professional presentations, the National Cybersecurity Workforce Framework, and private sector reports. In response to the 2011 GAO report, *Cybersecurity Human Capital*, a number of Federal agencies developed materials identifying characteristics specific to the cybersecurity profession. Additionally, the National Cybersecurity Workforce Framework puts forth a working taxonomy and common lexicon for cybersecurity workforce that can be overlaid onto any organization's existing occupational structure or roles[xvii]. Leading industry organizations echoed a number of these requirements through discussions on hiring challenges for both the private sector and academia[6]. Summarized below are the diverse characteristics or attributes that build the overarching cybersecurity workload and workforce requirements specific to cybersecurity professionals:

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

To provide a more complete understanding of these requirements, the analysis below expands on various perspectives on the cybersecurity workforce.

During times of crisis, cybersecurity workload priorities must be able to adjust from a steady-state operating environment to a ***surge capacity***. Therefore, cybersecurity professionals must be able to participate in surge situations like Denial of Service or virus attacks. The Navy Cyber/IT Workforce Strategic Plan describes cyberspace as a decentralized domain typified by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously,

6 The discussions involved Ronald Woerner, assistant professor at the College of Information Technology at Bellevue University; Dave Merkel, Chief Technology Officer of Mandiant; Derek Manky, senior security strategist at Fortinet; Shane Bernstein, managing partner of Q, an IT staffing agency; and Steve Santorelli of Team Cymru.

and inexpensively. This dynamic workload need precipitates most of the workforce requirements specific to cybersecurity professionals.

Cybersecurity requires its professionals to be ready to respond instantly to threats as soon as they are detected – the knowledge and ability to act in a variety of functions is closely linked to the capacity to surge and support efforts as needed in real time settings. Recognizing this, the Department of Defense established a set of cybersecurity requirements through the Information Enterprise Strategic Plan 2010-2012 that identified a need to develop a cybersecurity workforce to face both normal and *surge* operations, sometimes simultaneously[xviii]. To maintain high performance during steady times and effective support during a workload surge, the cybersecurity workforce must be ***agile***. A cybersecurity professional must have a broad knowledge base and range of skills and capacity to ***function in a variety of activities***.

In addition to supporting surge requirements, the cybersecurity workforce must also be able to exhibit a range of technical abilities, while retaining a willingness to work in a dispersed environment and remain extremely collaborative to support ***complex*** cybersecurity workload requirements. The Institute of Electrical and Electronics Engineers (IEEE) found that cybersecurity work includes analysis of policy, trends, and intelligence to better understand how an adversary may think or act - using problem-solving skills often compared to those of a detective[xix]. This level of work complexity requires the cybersecurity workforce to not only have a wide array of technical IT skills but also to possess advanced analysis capabilities.

The cybersecurity field not only faces complex situations during short-term threats, the work is consistently characterized as ***fast-paced*** and ***transformative***. This type of workload requires a workforce that is ***dynamic*** and ***flexible***. The IEEE states that cybersecurity professionals need to be those who can see themselves in fast-paced, busy environments, as well as people who understand that their job hours might be a bit unpredictable[xx]. Organizations should plan for regular or more frequent turnover due to this group's need to constantly learn new skills and improve their knowledge in other specialty areas. Those moves may be vertical through promotion or lateral from position to position. The nature of technology, both in innovation and development of new threats, dictates regular education and certification for the cybersecurity workforce.[xxi] To meet cybersecurity workload and workforce needs, organizations will need to establish protocols to allow the cybersecurity workforce to move easily between areas of practice.

Also representing the ***transformative*** workload is the field's maturity – cybersecurity hit its evolutional prime in the last 10 years, and continues to introduce new technology almost daily. Like all workload requirements, this also affects cybersecurity workforce requirements. The transformative nature of the work is providing for varying career paths – establishing a workforce with different educational backgrounds, an interest in innovative problem-solving, and a higher-than-average percentage of young professionals. This group thrives in an ***informal atmosphere*** of casual dress, unconventional working hours, and shifting work responsibilities aimed at keeping knowledge fresh and work exciting. To plan for the recruitment, development, and retention of these individuals, organizations will need to consider nontraditional hiring practices, less formal working environments, and flexible working schedules.

For workload planning, the requirements of surge capacity, speed, transformation, and high complexity must be considered and for workforce planning, requirements like agility, multi-functional, dynamic, flexible, and informal must be incorporated to achieve professional growth in

the field. To successfully address gaps and forecast future demand, the workforce planning approach developed in this field must address these unique requirements.

Conclusion

The cybersecurity community has reached a stage in its maturity making it capable of forecasting the future demand for the cybersecurity workforce. The research presented in this report serves as a foundation to encourage future discussion as NICE works in partnership with Federal state, local, tribal and territorial governments, industry, and academia to develop workforce planning approaches for the cybersecurity field.

Moving forward, organizations should base their cybersecurity workforce planning on the best practices of ***process, strategy, and infrastructure***:

- A consistent ***model*** for collecting and ***analyzing*** workforce ***data***
- *A* ***Vision*** of where the workforce planning capability is going in order to monitor ***performance*** and implement ***governance*** to ensure accuracy
- A strong understanding of how ***people*** and ***technology*** in the workforce ***collaborate*** together
- An analysis and understanding of the cybersecurity ***requirements*** specific to the workforce and workload

Specific to cybersecurity, successful workforce planning will employ risk assessments, customizable analysis tools, close monitoring of changes in skill sets, and agility to make quick course corrections. Risk assessment will be critical to forecasting a cybersecurity workforce because of the importance of the workload and related workforce role. Understanding how much risk is tolerable when planning for cybersecurity will allow organizations to understand the infrastructure, financial, and physical risks if the workforce is not appropriately staffed. In addition, requirements for cybersecurity are changing rapidly, placing supply and demand in constant flux– thereby making continuous monitoring for gap analysis data necessary for effective workforce planning. To both further mitigate risks and address the dynamic nature of cybersecurity, customizable analysis will be necessary to quickly understand the impact of work and workforce changes on the organization and better manage fluctuations in need.

While this paper begins to identify specific cybersecurity workload and workforce requirements, deeper analysis is a necessary next step. As an ever evolving and complex field, analysis of cybersecurity requirements will ensure that all workload and workforce requirements are identified and integrated into any workforce planning approach for cybersecurity planning.

Given the distinctive attributes of cybersecurity, and the breadth of organizational approaches to workforce planning, a next step in the evaluation of workforce planning for the cybersecurity field should be the development of a best-practices driven cybersecurity workforce planning approach that integrates the specific best practices identified here with the taxonomy of The National Cybersecurity Workforce Framework. Equally important will be the need to further define, analyze, and understand the unique cybersecurity workload and workforce requirements that will enable a focused and accurate workforce planning method for the cybersecurity field. Additionally, a Capability Maturity Model (CMM) should be developed to allow organizations to self-identify their stage in workforce planning and make necessary adjustments to improve planning efforts for their cybersecurity workforce and workload.

Appendix A. Acronyms

Acronym	Definition
COP	Community of Practice
CMM	Capability Maturity Model
CNCI	Comprehensive National Cybersecurity Initiative
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
GAO	General Accountability Office
HR	Human Resources
HRIS	Human Resource Information Systems
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
NASA	National Aeronautics and Space Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency

Appendix B. References

[i] "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually." September 7, 2011. http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

[ii] Ibid.

[iii] "The National Cybersecurity Workforce Framework." National Initiative for Cybersecurity Education. 2011. http://csrc.nist.gov/nice/framework/

[iv] "In the Dark: Crucial Industries Confront Cyberattacks," a report commissioned by McAfee and written by Center for Strategic & International Studies (CSIS), 2011.

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

[vi] "Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination." GAO-12-8. November 2011. http://www.gao.gov/assets/590/586494.pdf.

[vii] "Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce." Partnership for Public Service. July 2009.

[viii] "The CERT® Approach to Cybersecurity Workforce Development." Software Engineering Institute. December 2010.

[ix] "Second Annual Cost of Cyber Crime Study." Ponemon Institute, LLC. August 2011 http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

[x] "An Operational Process for Workforce Planning." RAND. 2005. http://www.rand.org/pubs/monograph_reports/2005/MR1684.1.pdf

[xi] "Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce." Partnership for Public Service. July 2009.

[xii] "Stevelman, Ruth and Rachele Williams, et al., "Strategic Work Force Planning: Anticipating and Filling Talent Gaps, Best Practices Report." Houston: AQPC, 2009.

[xiii] "Evaluating Workforce Needs, Government Performance Project, Washington, D.C." The Pew Center on the States, 2010.

[xiv] "Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination." GAO-12-8. November 2011. http://www.gao.gov/assets/590/586494.pdf.

[xv] Ibid.

[xvi] Wikipedia definition

[xvii] "The National Cybersecurity Workforce Framework." National Initiative for Cybersecurity Education. 2011. http://csrc.nist.gov/nice/framework/

[xviii] Ibid.

[xix] Platt, John R. "Career Focus: Cyber Security- A Growing Threat, a Growing Career." Today's Engineers, August 2011. http://www.todaysengineer.org/2011/Aug/career-focus.asp

[xx] Ibid.

[xxi] Ibid.

Contact Information:
Kristina Dorville
Branch Chief, Cyber Education & Awareness
Department of Homeland Security (DHS)
Email: Kristina.Dorville@HQ.DHS.GOV
Phone:703-235-5761