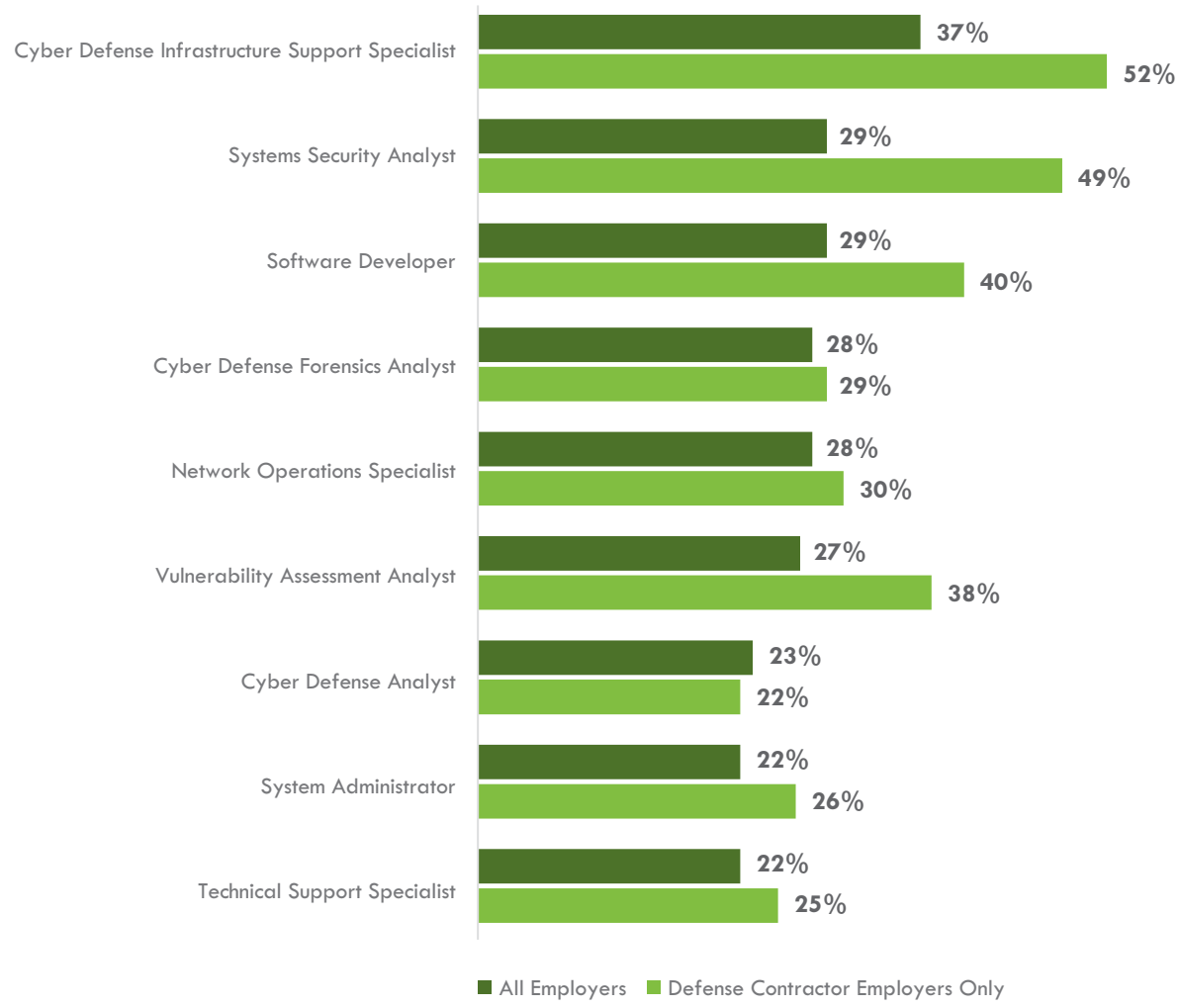
CANDIDATE CHALLENGES

Lack of Security Clearances

The top three work roles for which candidates lack necessary security clearances are the same for all employers and defense contractors: cyber defense infrastructure support specialist, systems security analyst and software developer (Exhibit 16).

Finding qualified candidates with the necessary security clearances is on average more of a challenge for defense contractors. For example, for systems security analysts the percentage of defense contractors reporting this challenge is 49%, which is 20% higher than employers in the overall sample.

Exhibit 16. Lack of candidates with necessary security clearances, all employers and defense contractors

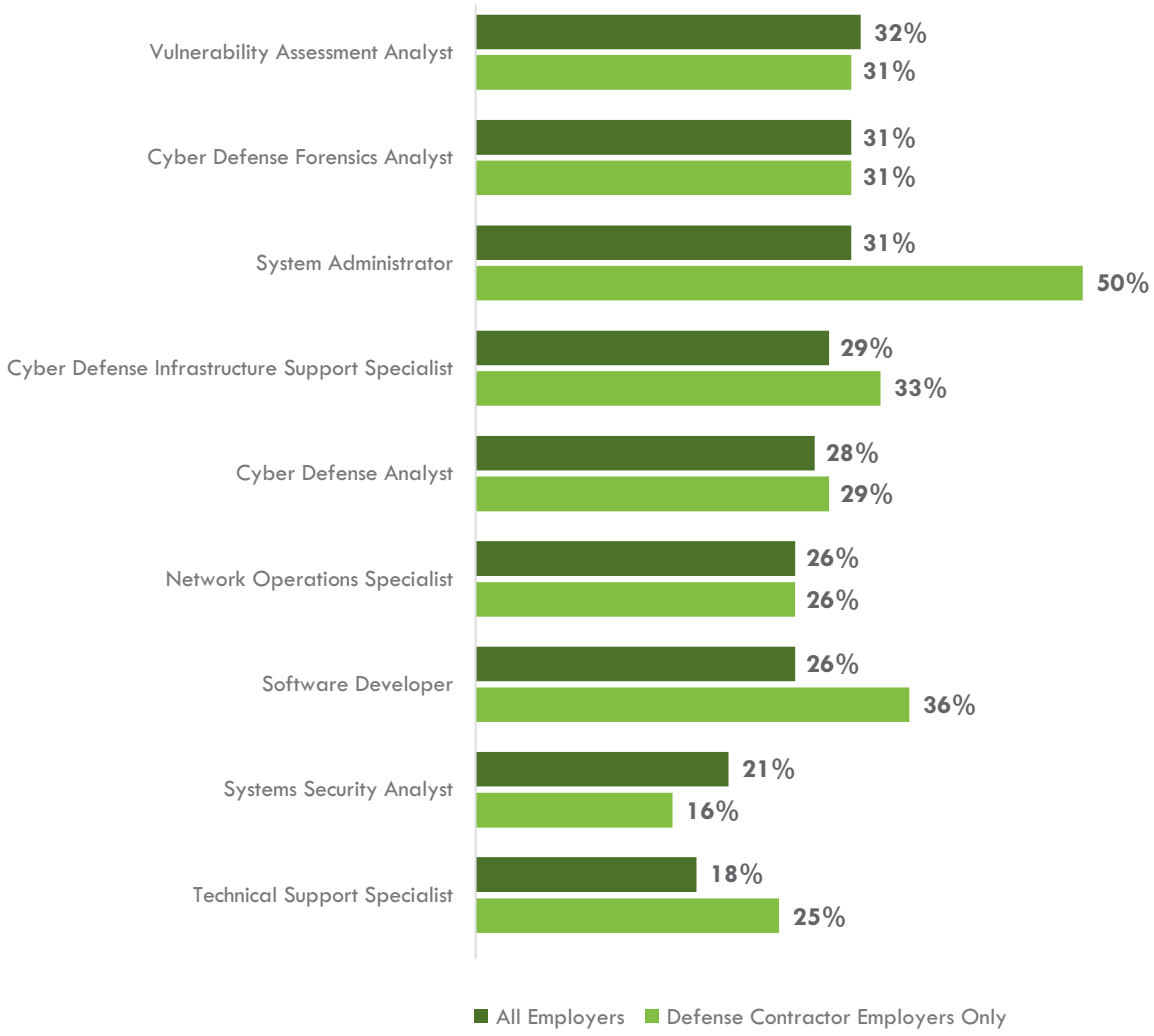


CANDIDATE CHALLENGES

Lack of Education

Defense contractors as a subgroup varied from employers in the overall sample in reporting which work roles lacked candidates with the required educational attainment (Exhibit 17). Vulnerability assessment analyst was the most common work role for all employers, while system administrator was the most common for defense contractors.

Exhibit 17. Lack of required educational attainment for work roles reported by all employers and defense contractors



SECURITY CERTIFICATIONS

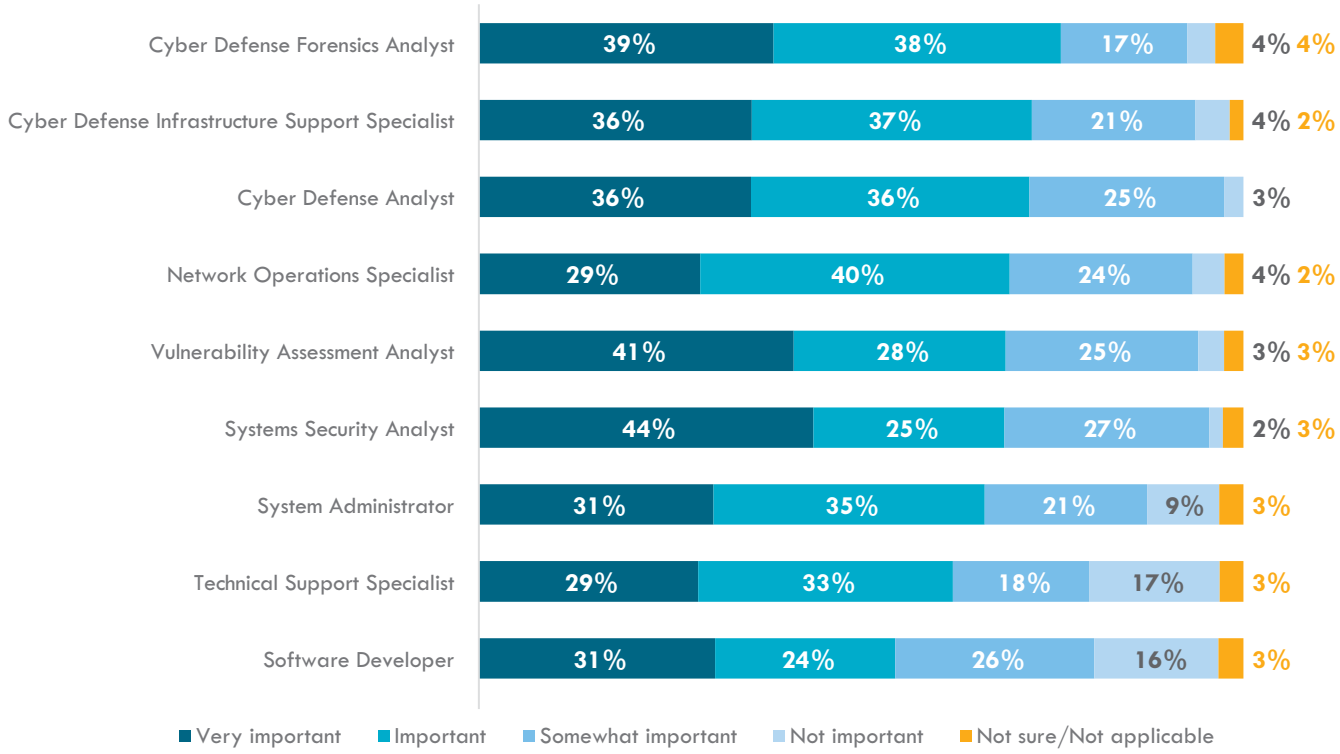
Employers were asked how important a security certification is when hiring for each of the nine work roles. The number of employers who responded to this question ranged from 109 to 129, depending on the work role.

For all nine work roles, 55% or more of employers reported that security certifications are important or very important when hiring (Exhibit 18). For seven of the nine work roles, 66% or more of employers reported that security certifications are important or very important when hiring.

Work roles for which employers reported security certifications are important include:

- 77% of employers reported that when hiring for cyber defense forensics analysts a security certification was important or very important.
- 73% of employers indicated that when hiring for cyber defense infrastructure support specialists a security certification was important or very important.
- 72% of employers reported that when hiring for cyber defense analysts a security certification was important or very important.

Exhibit 18. Level of importance of security certifications reported by employers for the nine work roles



SECURITY CERTIFICATIONS

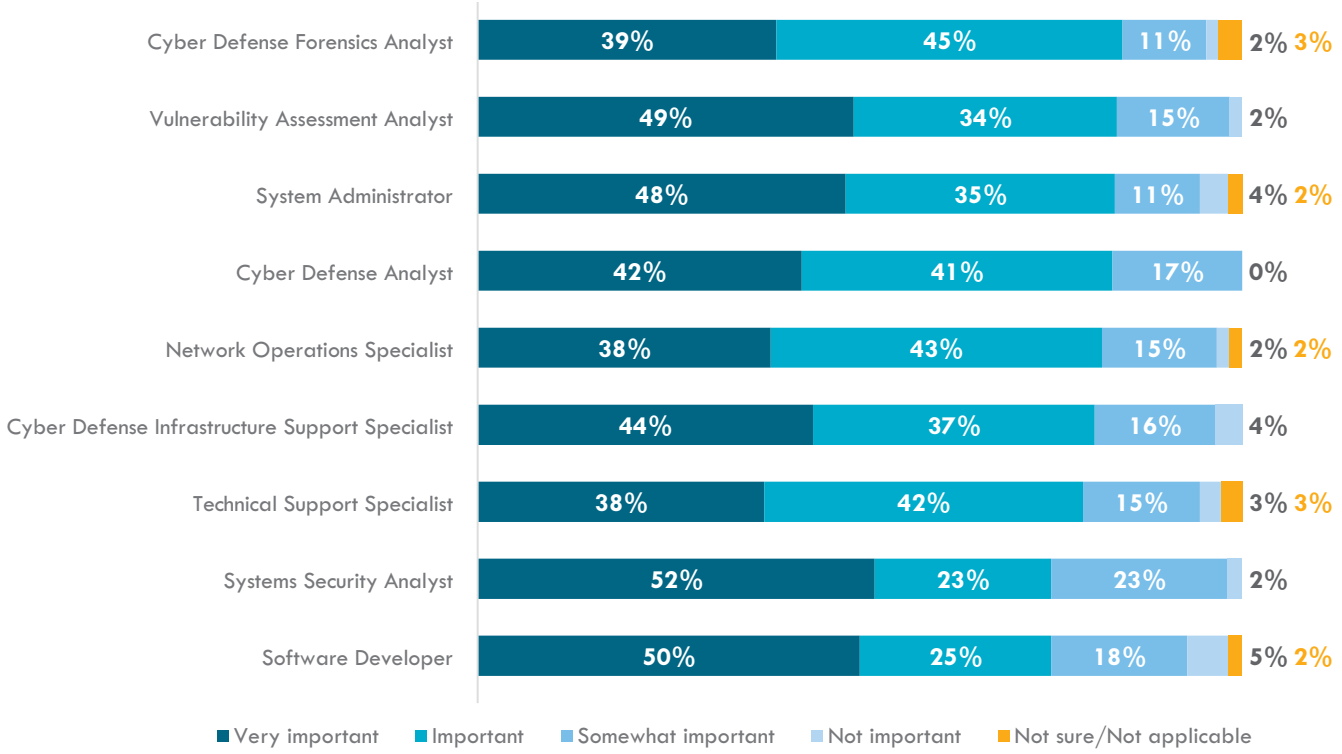
For all nine work roles, 75% or more of defense contractors reported that security certifications are important or very important when hiring (Exhibit 19). Security certifications appear to be more important to defense contractors than to the overall sample of employers who responded to this question. The number of defense contractors who responded to this question ranges from 52 to 72 depending on the work role.

For seven of the nine work roles, 80% or more of defense contractors reported that security certifications are important or very important when hiring.

Work roles for which defense contractors reported security certifications are important include:

- 84% of defense contractors reported that when hiring for cyber defense forensics analysts a security certification was important or very important.
- 83% of defense contractors indicated that when hiring for vulnerability assessment analysts a security certification was important or very important.
- 83% of defense contractors reported that when hiring for system administrators a security certification was important or very important.
- 83% of defense contractors reported that when hiring for cyber defense analysts a security certification was important or very important.

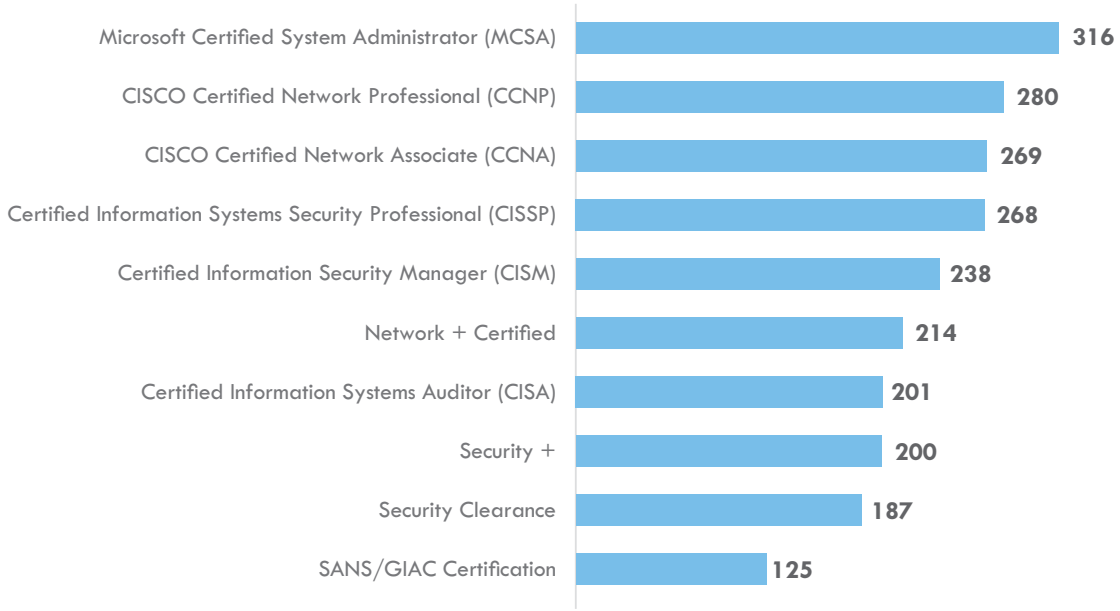
Exhibit 19. Level of importance of security certifications reported by defense contractors for the nine work roles



SECURITY CERTIFICATIONS

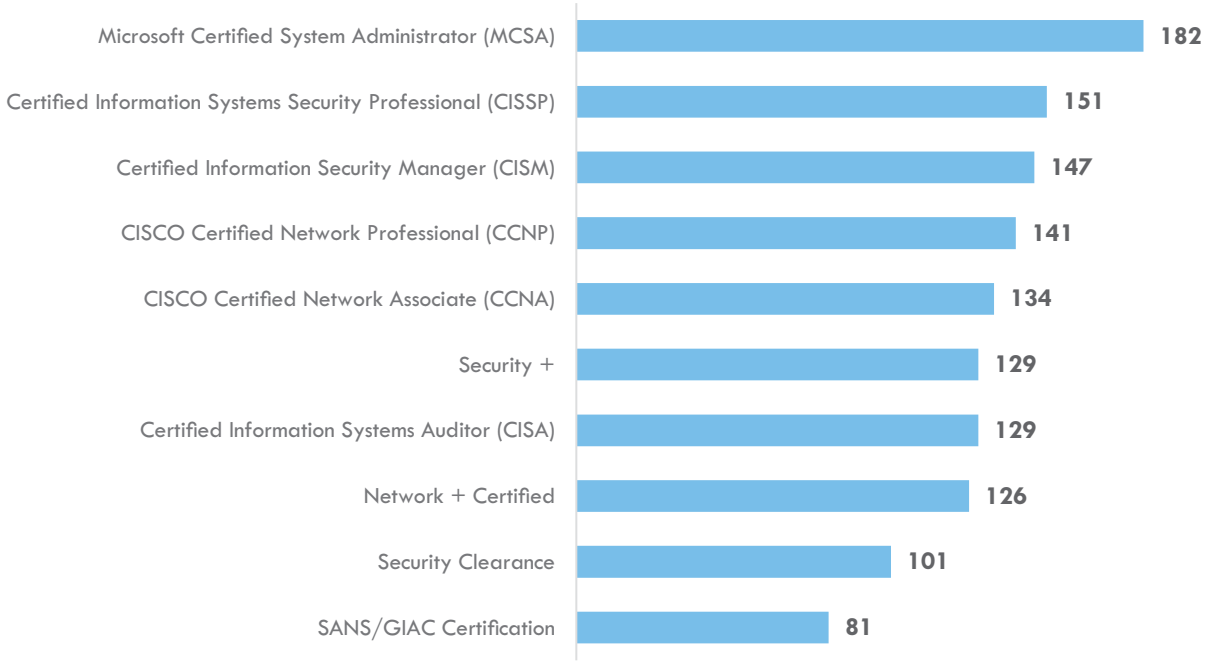
Respondents who answered that a security certification was important or very important were asked to select the certification(s) they prefer from a list of options; they could select all certifications that applied. Exhibit 20 shows the aggregate responses across all nine work roles. Results for the security certifications preferred for each work role are displayed in Appendix D in the work role profiles.

Exhibit 20. Security certifications preferred, all employers



Defense contractors who answered that a security certification was important or very important, were asked to select the certification(s) they prefer from a list of options; they could select all certifications that applied. Exhibit 21 shows the aggregate responses across all nine work roles reported by defense contractors.

Exhibit 21. Security certifications preferred, defense contractors



IMPORTANCE OF CYBERSECURITY SKILLS FOR IT/IS WORK ROLES

The high percentage of employers indicating these skills are important or very important provides validation of the skills in the NICE Framework.

Increasingly IT/IS workers need cybersecurity skills related to their work roles. Utilizing the NICE Framework, specific cybersecurity skills were identified from among the complete list of skills in the framework, for each of the following work roles: technical support specialist, network operations specialist, system administrator, and software developer.

Employers were asked to rate the importance of each cybersecurity specific skill for work roles they have at their business. The results below show the percentage of employers who indicated each skill was important or very important for the work role. The high percentage of California employers indicating these skills are important or very important provides validation of the cybersecurity specific skills outlined in the NICE Framework, for these four work roles.

Technical Support Specialist

Finding: For three of the four cybersecurity skills, 78% or more of employers indicated they are important or very important.

Skill: Accurately defining incidents, problems, and events in the trouble ticketing system. (84%)

Skill: Using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. (83%)

Skill: Identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation. (78%)

Skill: Designing incident response for cloud service models. (67%)

Network Operations Specialist

Finding: For all six cybersecurity skills, 80% or more of employers indicated they are important or very important.

Skill: Protecting a network against malware (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). (88%)

Skill: Configuring and utilizing network protection components (e.g., firewalls, VPNs, network intrusion detection systems). (88%)

Skill: Implementing, maintaining, and improving established network security practices. (86%)

Skill: Securing network communications. (85%)

Skill: Configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). (83%)

Skill: Implementing and testing network infrastructure contingency and recovery plans. (80%)

IMPORTANCE OF CYBERSECURITY SKILLS FOR IT/IS WORK ROLES

Systems Administrator

Finding: For all four cybersecurity skills, 82% or more of employers indicated they are important or very important.

Skill: Accurately define incidents, problems, and events in the trouble ticketing system. (89%)

Skill: Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (88%)

Skill: Configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). (85%)

Skill: Establishing and maintaining automated security control assessments. (82%)

Software Developer

Finding: For five of the seven cybersecurity skills, 68% or more of employers indicated they are important or very important.

Skill: Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (76%)

Skill: Developing and applying security system access controls. (70%)

Skill: Using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (70%)

Skill: Secure test plan design (e.g., unit, integration, system, acceptance). (69%)

Skill: Designing countermeasures to identified security risks. (68%)

Skill: Discerning the protection needs (i.e., security controls) of information systems and networks. (64%)

Skill: Conducting vulnerability scans and recognizing vulnerabilities in security systems. (61%)

A very high percentage of defense contractors also rated the NICE Framework cybersecurity skills for the four work roles as important or very important. The number of defense contractors who responded to this question ranged from 52 to 72 depending on the work role.

Based on responses from defense contractors, key findings for each work role include:

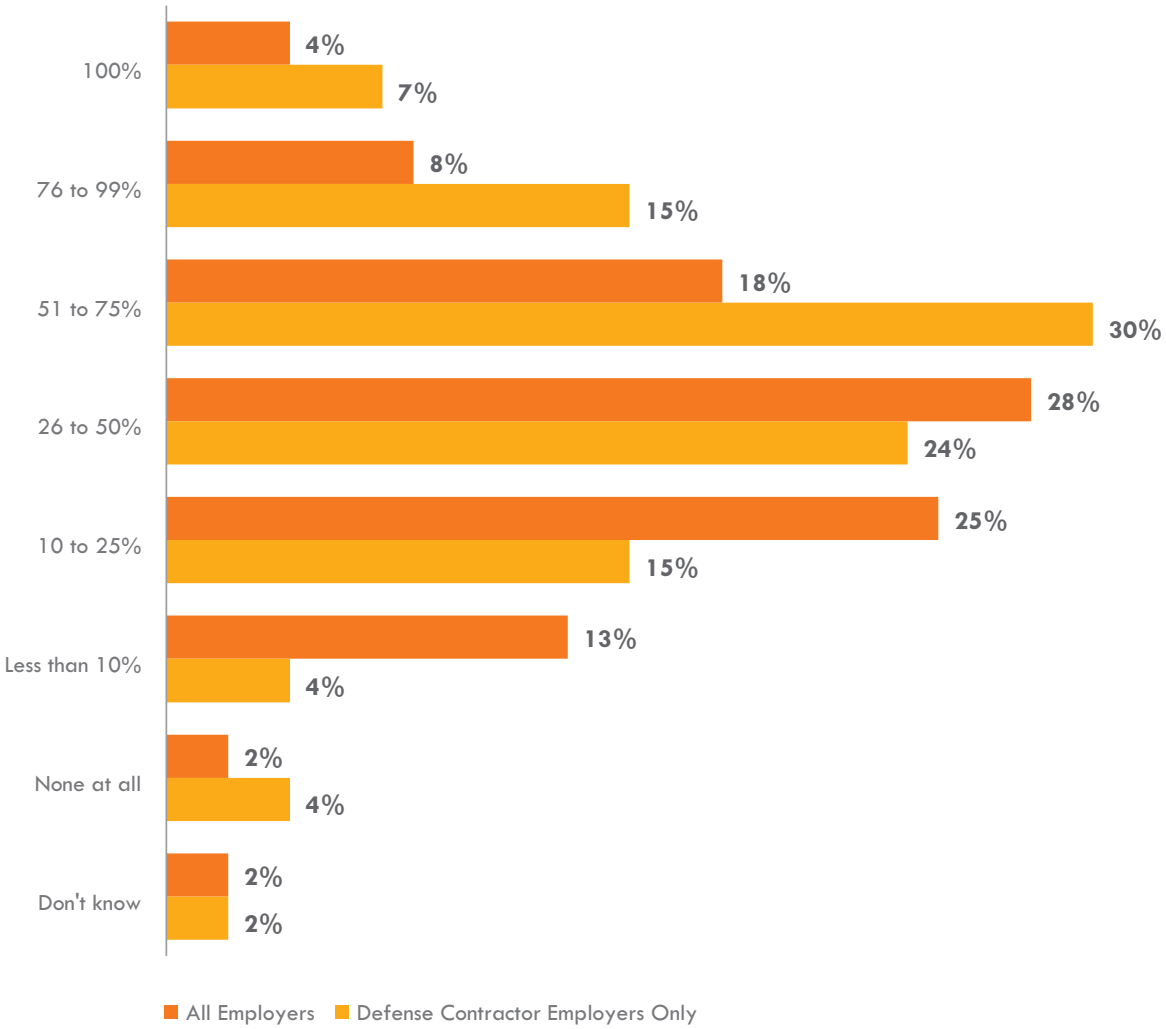
- Technical support specialist—For all four cybersecurity skills, 79% or more of defense contractors indicated they are important or very important.
- Network operations specialist—For all six cybersecurity skills, 82% or more of defense contractors indicated they are important or very important.
- Systems administrator—For all four cybersecurity skills, 80% or more of defense contractors indicated they are important or very important.
- Software developer—For all seven cybersecurity skills, 68% or more of defense contractors indicated they are important or very important.

TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

For the same four IT/IS work roles that require cybersecurity skills, employers were asked to document on average, the percentage of time (within the overall job duties) spent on security/cybersecurity issues. Compared to employers in the overall sample, the percentage of defense contractors indicating that employees spend more than a quarter of their time on security/cybersecurity issues is higher by between 17% and 23%, depending on the work role.

Exhibit 22 shows that 58% of employers in the overall sample compared to 76% of defense contractors said that system administrators spend more than a quarter of their time on security/cybersecurity issues.

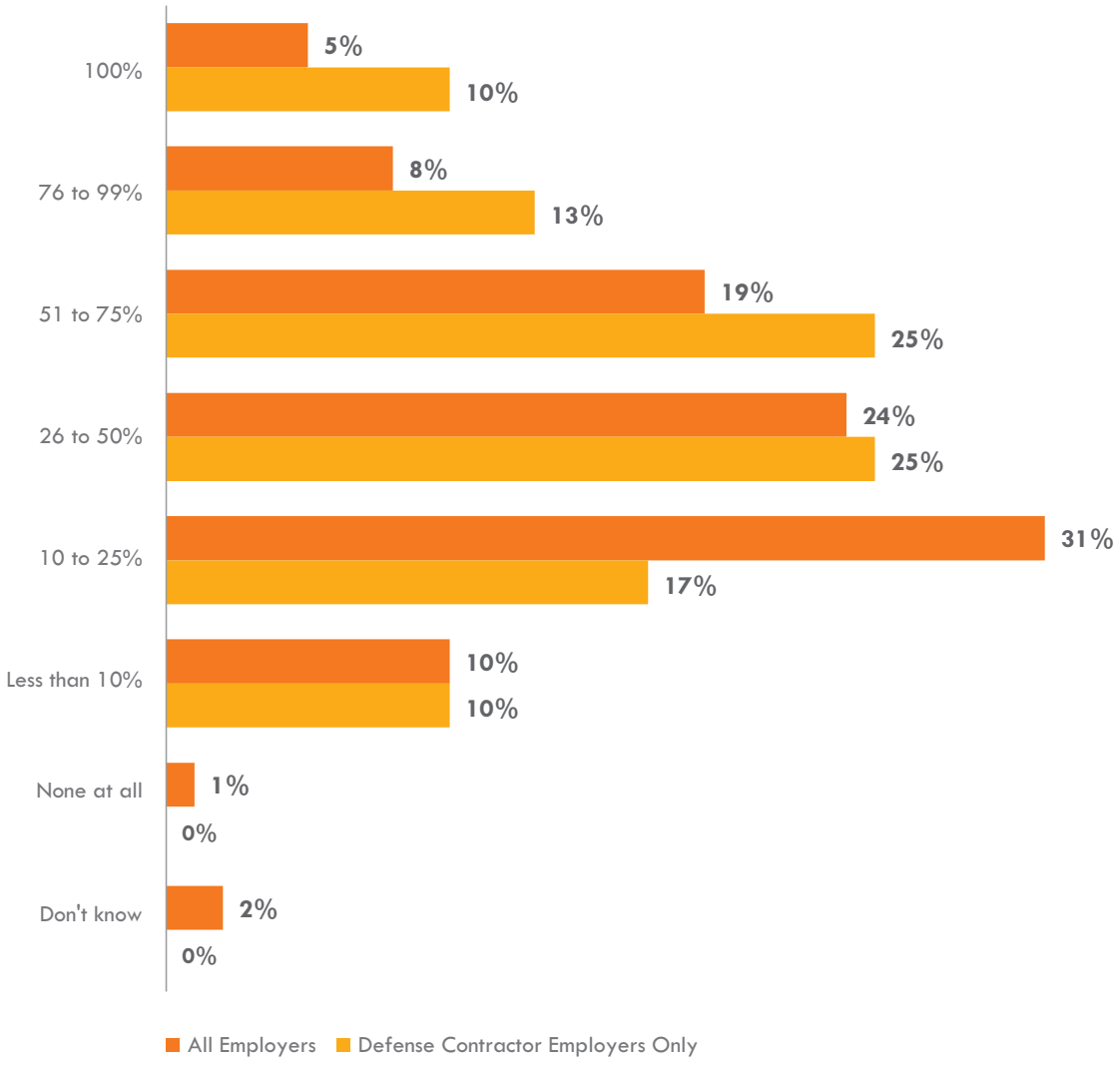
Exhibit 22. Percentage of time systems administrators spend on security/ cybersecurity issues, all employers and defense contractors



TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

Exhibit 23 shows 56% of all employers compared to 73% of defense contractors said that network operations specialists spend more than a quarter of their time on security/cybersecurity issues.

Exhibit 23. Percentage of time network operations specialists spend on security/ cybersecurity issues, all employers and defense contractors



TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

Exhibit 24 shows that 55% of employers compared to 73% of defense contractors said that technical support specialists spend more than a quarter of their time on security/cybersecurity issues.

Exhibit 24. Percentage of time technical support specialists spend on security/ cybersecurity issues, all employers and defense contractors