Writing Cybersecurity Position Descriptions for the Greatest Impact

January 17, 2018
RecruitHer

Writing job descriptions that resonate
RecruitHer will help companies recruit more female applicants and increase their presence in tech and STEM related fields.
The Problem

9 out of 10 hiring managers and recruiters report finding and hiring tech workers to be one of their biggest challenges.*

Fewer than 25% of tech jobs are held by women.**

Diversity promotes more creativity, better problem solving, and innovation.**

* 2017 Indeed Hiring Survey
** 2016 Annual Report, National Center for Women and Information Technology
Talent Acquisition Challenge

Job descriptions communicate what the organization demands from the potential employee.

Job descriptions focus on the needs of the candidates—a tactic that yields three times as many highly-rated applicants*

* Global Human Capital Trends 2017 - Deloitte
Unconscious bias in job postings discourages women from applying.
When job advertisements were constructed to include more masculine than feminine wording:

- participants perceived more men within these occupations,
- women found these jobs less appealing, and
- perceptions of belongingness—**not perceived skills**—mediated the effect of gendered wording on job appeal.

RecruitHer analyzes job postings for gendered language and makes data driven recommendations for alternative language.
How Do We Do It?

- **Domain specific data:** *Actual resumes of actual tech talent*
- **Cutting-edge machine learning:** Deep learning and neural networks
- **Context-based recommendations:** *Discover the words that resonate*
Real Results

We are looking for a confident and extremely motivated developer that enjoys difficult challenges. Ability to think critically and drive innovation in a team development environment are required.

We are looking for a confident and energetic developer that enjoys new challenges. Ability to think creatively and proactively for success in a team development environment are required.
RecruitHer’s recommendations led to:

- 4% increase in male applicants
- 15% increase in female applicants
Q & A
Welcome

Writing Cybersecurity Job Descriptions for the Greatest Impact

Keith T. Hall
U.S. Department of Homeland Security
Disclaimers and Caveats

• **Content Not Officially Adopted.** The content of this briefing is mine personally and does not reflect any position or policy of the United States Government (USG) or of the Department of Homeland Security.

• **Note on Terminology.** Will use USG terminology in this brief (but generally translatable towards Private Sector equivalents)

• **Job Description Usage.** For the purposes of this presentation only, the Job Description for the Position Description (PD) is used synonymously with the Job Opportunity Announcement (JOA). Although there are potential differences, it is not material to the concepts presented today.
Key Definitions and Concepts

• **What do you want the person to do?**

  • **Major Duties and Responsibilities.** “A statement of the important, regular, and recurring duties and responsibilities assigned to the position”  

  • **Major vs. Minor Duties.** “Major duties are those that represent the primary reason for the position's existence, and which govern the qualification requirements. Typically, they occupy most of the employee's time. Minor duties generally occupy a small portion of time, are not the primary purpose for which the position was established, and do not determine qualification requirements”  

  • **Tasks.** “Activities an employee performs on a regular basis in order to carry out the functions of the job.”  
• **What do you want to see on resumes that qualifies them to do this work?**

• **Competency.** “Competency is a **measurable pattern of knowledge, skills, abilities (KSAs), behaviors,** and other characteristics that an individual needs to perform work roles or occupational functions successfully. Competencies specify the ‘how’ of performing job tasks, or what the person needs to do the job successfully.”  


  o **Behaviors** – “the way in which one acts or conducts oneself, especially toward others”
  o **Knowledge** – “facts, information, and skills acquired by a person through experience or education; the *theoretical or practical* understanding of a subject”
  o **Abilities** – “possession of the means or skill to do something”
  o **Skills** – “the ability to do something well; expertise”
Where to start?

I want to hire someone..
Why Start Here?

• "What’s the problem? – I’ll just put out my old announcement until I get the right candidate."
  • Did the position require a skill not listed on the announcement?
  • How much end-to-end time or resources will be wasted running through the responses?

• "I don’t have to hire anyone, I just need to outsource the work."
  • Don’t you still need to articulate your requirements into the contract?
  • Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

• "I keep reading about the cyberskills gap, but I don’t see how it’s any different from non-cyber positions."
  • True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  • It seems easy, but it’s not..
Why Start Here?

• “What’s the problem? – I’ll just put out my old announcement until I get the right candidate..”
  • Did the position require a skill not listed on the announcement?
  • How much end-to-end time or resources will be wasted running through the responses?

• “I don’t have to hire anyone, I just need to outsource the work..”
  • Don’t you still need to articulate your requirements into the contract?
  • Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

• “I keep reading about the cyberskills gap, but I don’t see how it’s any different from non-cyber positions?”
  • True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  • It seems easy, but it’s not..
Why Start Here?

• “What’s the problem? – I’ll just put out my old announcement until I get the right candidate..”
  • Did the position require a skill not listed on the announcement?
  • How much end-to-end time or resources will be wasted running through the responses?

• “I don’t have to hire anyone, I just need to outsource the work..”
  • Don’t you still need to articulate your requirements into the contract?
  • Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

• “I keep reading about the cyberskills gap, but I don’t see how it’s any different from non-cyber positions?”
  • True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  • It seems easy, but it’s not..
Why Start Here?

• “What’s the problem? – I’ll just put out my old announcement until I get the right candidate..”
  • Did the position require a skill not listed on the announcement?
  • How much end-to-end time or resources will be wasted running through the responses?

• “I don’t have to hire anyone, I just need to outsource the work..”
  • Don’t you still need to articulate your requirements into the contract?
  • Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

• “I keep reading about the cyberskills gap, but I don’t see how it’s any different from non-cyber positions?”
  • True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  • It seems easy, but it’s not..
Why Start Here?

• “What’s the problem? – I’ll just put out my old announcement until I get the right candidate..”
  • Did the position require a skill not listed on the announcement?
  • How much end-to-end time or resources will be wasted running through the responses?

• “I don’t have to hire anyone, I just need to outsource the work..”
  • Don’t you still need to articulate your requirements into the contract?
  • Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

• “I keep reading about the cyberskills gap, but I don’t see how it’s any different from non-cyber positions?”
  • True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  • It seems easy, but it’s not..
Why Start Here?

• “What’s the problem? – I’ll just put out my old announcement until I get the right candidate..”
  • Did the position require a skill not listed on the announcement?
  • How much end-to-end time or resources will be wasted running through the responses?

• “I don’t have to hire anyone, I just need to outsource the work..”
  • Don’t you still need to articulate your requirements into the contract?
  • Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

• “I keep reading about the cyberskills gap, but I don’t see how it’s any different from non-cyber positions?”
  • True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  • It seems easy, but it’s not..
Why is a Job Description So Important?

• **Tactical Reason**: “I meant what I said and I said what I meant.”  
  SOURCE: Dr. Seuss, Horton Hatches and Egg, Random House, 1940
  - Accuracy in the Job Opportunity Announcement (JOA)
  - Clearly communicates intent *directly* to Job Candidates
  - Overall better Job Candidate quality in response

• **Strategic Reason**: Proactive Workforce Planning
  - Can future plans be supported with *existing* skillsets?
  - What new skillsets are required?
  - What is the current gap in delivery capability that re-training current workforce cannot achieve in sufficient time or in quantity?
Why is a Job Description So Important?

• **Tactical Reason**: “I meant what I said and I said what I meant.”
  SOURCE: Dr. Seuss, Horton Hatches and Egg, Random House, 1940
  • Accuracy in the Job Opportunity Announcement (JOA)
  • Clearly communicates intent *directly* to Job Candidates
  • Overall better Job Candidate quality in response

• **Strategic Reason**: Proactive Workforce Planning
  • Can future plans be supported with *existing* skillsets?
  • What new skillsets are required?
  • What is the current gap in delivery capability that re-training current workforce cannot achieve in sufficient time or in quantity?
Why is a Job Description So Important?

• **Tactical Reason**: “I meant what I said and I said what I meant.”

  SOURCE: Dr. Seuss, Horton Hatches and Egg, Random House, 1940

  • Accuracy in the Job Opportunity Announcement (JOA)
  • Clearly communicates intent *directly* to Job Candidates
  • Overall better Job Candidate quality in response

• **Strategic Reason**: Proactive Workforce Planning

  • Can future plans be supported with *existing* skillsets?
  • What new skillsets are required?
  • What is the current gap in delivery capability that re-training current workforce cannot achieve in sufficient time or in quantity?
About Job Description Alignment (Tactical Example)

- **MAJOR DUTY**
- **TASK**
- **What the Manager expects the candidate to perform on the job.**
- **KNOWLEDGE, SKILL, ABILITY**
- **Knowledge, Skill, Ability**
- **May be OJT or something the candidate can learn in a short amount of time (i.e. 90 days)**
- **Most closely aligned to announcement questionnaires, retention bonuses, retraining efforts, etc.**
- **Something the candidate brings to the table that *CANNOT* be easily learned in a short amount of time (i.e. 90 days)**
- **The combination of experience, education, training, certification and special circumstances that formed knowledge, skills, or abilities.**
- **JOB EXPERIENCE**
- **EDUCATION**
- **TRAINING**
- **CERTIFICATION**
- **SPECIAL CIRCUMSTANCE**

Documented via resume and applicant’s questionnaire responses.
About Job Description Alignment (Tactical Example)
About Job Description Alignment (Tactical Example)

- **MAJOR DUTY**
  - What the Manager expects the candidate to perform on the job.
  - What the candidate is responsible for or responsible to perform in the job position.
  - May be OJT or something the candidate can learn in a short amount of time (i.e. 90 days)

- **TASK**
  - KNOWLEDGE, SKILL, ABILITY
  - KNOWLEDGE, SKILL, ABILITY
  - KNOWLEDGE, SKILL, ABILITY

- **KNOWLEDGE, SKILL, ABILITY**
  - Most closely aligned to announcement questionnaires, retention bonuses, retraining efforts, etc.

- **JOB EXPERIENCE**
- **EDUCATION**
- **TRAINING**
- **CERTIFICATION**
- **SPECIAL CIRCUMSTANCE**

The combination of experience, education, training, certification and special circumstances that formed knowledge, skills, or abilities.

Documented via resume and applicant’s questionnaire responses.
About Job Description Alignment (Tactical Example)

What the candidate is responsible for or responsible to perform in the job position.

What the Manager expects the candidate to perform on the job.

Most closely aligned to announcement questionnaires, retention bonuses, retraining efforts, etc.

The combination of experience, education, training, certification and special circumstances that formed knowledge, skills, or abilities.

May be OJT or something the candidate can learn in a short amount of time (i.e. 90 days)

Something the candidate brings to the table that *CANNOT* be easily learned in a short amount of time (i.e. 90 days)

Documented via resume and applicant’s questionnaire responses.
About the Dynamics of Hiring
About the Dynamics of Hiring

I want to interview qualified candidates.
About the Dynamics of Hiring

I want this job

I want to interview qualified candidates
The Experience, Education, Training and Certification Ecosystem
Cyber Positions, Skillset Attributes & Elements (Some Examples)

• **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.

• **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.


• **Proficiency Level.** Ex. Basic, Journeyman, Advanced.

• **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).

• **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.

• **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Cyber Positions, Skillset Attributes & Elements (Some Examples)

- **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.
- **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.
- **Proficiency Level.** Ex. Basic, Journeyman, Advanced.
- **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).
- **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.
- **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Cyber Positions, Skillset Attributes & Elements (Some Examples)

- **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.

- **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.


- **Proficiency Level.** Ex. Basic, Journeyman, Advanced.

- **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).

- **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.

- **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Cyber Positions, Skillset Attributes & Elements (Some Examples)

- **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.
- **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.
- **Proficiency Level.** Ex. Basic, Journeyman, Advanced.
- **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).
- **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.
- **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology.
Cyber Positions, Skillset Attributes & Elements (Some Examples)

- **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.

- **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.


- **Proficiency Level.** Ex. Basic, Journeyman, Advanced.

- **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).

- **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.

- **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Cyber Positions, Skillset Attributes & Elements (Some Examples)

- **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.
- **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.
- **Proficiency Level.** Ex. Basic, Journeyman, Advanced.
- **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).
- **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.
- **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Cyber Positions, Skillset Attributes & Elements (Some Examples)

• **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.

• **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.


• **Proficiency Level.** Ex. Basic, Journeyman, Advanced.

• **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).

• **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.

• **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Cyber Positions, Skillset Attributes & Elements (Some Examples)

• **Offensive vs Defensive.** Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.

• **Proactive, Continuous, vs Reactive.** Ex. Security Engineer vs. Incident Responder.


• **Proficiency Level.** Ex. Basic, Journeyman, Advanced.

• **Technology Focus.** Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).

• **OJT (< 90d) vs Pre-Existing (> 90d).** Ex. Orientation vs. Core Skillset.

• **Specificity Level.** Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology
Vendor-Independent vs. Vendor-Specific 
Experience, Education, Training and Certifications

VENDOR-INDEPENDENT

ADVANTAGES:
• Fewer legal hurdles (Government Competition Standpoint)
• Covers Knowledge and Concepts

DISADVANTAGES:
• Hands-on time-to-operations can be > 90 days

VENDOR-SPECIFIC

ADVANTAGES:
• Hands-on time-to-operations can be < 90 days

DISADVANTAGES:
• Normally narrower in scope (may or may not provide direct applicability to the organization)
Vendor-Independent vs. Vendor-Specific Experience, Education, Training and Certifications

VENDOR-INDEPENDENT

ADVANTAGES:
• Fewer legal hurdles (Government Competition Standpoint)
• Covers Knowledge and Concepts

DISADVANTAGES:
• Hands-on time-to-operations can be > 90 days

VENDOR-SPECIFIC

ADVANTAGES:
• Hands-on time-to-operations can be < 90 days

DISADVANTAGES:
• Normally narrower in scope (may or may not provide direct applicability to the organization)
Vendor-Independent vs. Vendor-Specific Experience, Education, Training and Certifications

VENDOR-INDEPENDENT

ADVANTAGES:
• Fewer legal hurdles (Government Competition Standpoint)
• Covers Knowledge and Concepts

DISADVANTAGES:
• Hands-on time-to-operations can be > 90 days

VENDOR-SPECIFIC

ADVANTAGES:
• Hands-on time-to-operations can be < 90 days

DISADVANTAGES:
• Normally narrower in scope (may or may not provide direct applicability to the organization)
Training vs Certification Baselines

TRAINING

• **Entry / Basic-Level** (e.g. Taking the class or “I can learn from the book”; *knowledge of*)
• **Journeyman / Mid-Level** (e.g. Able to perform or “I can apply the book”; *skill or ability to*)
• **Mastery or Expert / Senior-Level** (e.g. Teaching the class or “I can teach others the book”; *expert in or mastery of*)
• **Senior Mastery-Expert / SME-Level** (e.g. authoring new materials or “I can write the book”). Ex. *Developing new material where no pre-existing material exists.*

CERTIFICATIONS

• **Vendor-Independent or Knowledge-Based Certifications** (represent a *minimum or baseline level of knowledge*)
  Analysis functions could be <90d; vendor-specific, *hands-on functions >90d*
• **Hands-on, Vendor-Specific Certifications**
  (represent a *minimum or baseline level of skill or ability*) Vendor-specific, *hands-on functions <90d*
Training vs Certification Baselines

**TRAINING**

- **Entry / Basic-Level** (e.g. Taking the class or “I can learn from the book”; *knowledge of*)
- **Journeyman / Mid-Level** (e.g. Able to perform or “I can apply the book”; *skill or ability to*)
- **Mastery or Expert / Senior-Level** (e.g. Teaching the class or “I can teach others the book”; *expert in or mastery of*)
- **Senior Mastery-Expert / SME-Level** (e.g. authoring new materials or “I can write the book”). Ex. *Developing new material where no pre-existing material exists.*

**CERTIFICATIONS**

- **Vendor-Independent or Knowledge-Based Certifications** (represent a *minimum or baseline level of knowledge*) Analysis functions could be <90d; vendor-specific, *hands-on functions >90d*
- **Hands-on, Vendor-Specific Certifications** (represent a *minimum or baseline level of skill or ability*) Vendor-specific, *hands-on functions <90d*
Training vs Certification Baselines

TRAINING

• Entry / Basic-Level (e.g. Taking the class or “I can learn from the book”; knowledge of)

• Journeyman / Mid-Level (e.g. Able to perform or “I can apply the book”; skill or ability to)

• Mastery or Expert / Senior-Level (e.g. Teaching the class or “I can teach others the book”; expert in or mastery of)

• Senior Mastery-Expert / SME-Level (e.g. authoring new materials or “I can write the book”). Ex. Developing new material where no pre-existing material exists.

CERTIFICATIONS

• Vendor-Independent or Knowledge-Based Certifications (represent a minimum or baseline level of knowledge) Analysis functions could be <90d; vendor-specific, hands-on functions >90d

• Hands-on, Vendor-Specific Certifications (represent a minimum or baseline level of skill or ability) Vendor-specific, hands-on functions <90d
# Specificity Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Category</th>
<th>Granularity</th>
<th>Example Content</th>
<th>Example Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>CATEGORY</td>
<td>Broad category</td>
<td>OPM MOSAIC (Cybersecurity)</td>
<td>Background or Foundational Knowledge Requirements; Internships</td>
</tr>
<tr>
<td>II</td>
<td>SUBCATEGORY</td>
<td>Workrole, Functional Area, Major Duty</td>
<td>NICE Framework; DoD AT&amp;L; FAI FAC; CIP</td>
<td>Non-hands-on positions; Generalists</td>
</tr>
<tr>
<td>III</td>
<td>TYPE</td>
<td>Specific Technologies, Devices or Programming Languages</td>
<td>Vendor-specific certifications, specific programming languages, or technology-specific coursework</td>
<td>Hands-on positions</td>
</tr>
<tr>
<td>IV</td>
<td>SUBTYPE</td>
<td>Specific Techniques, Specialties, or Research Areas</td>
<td>Specific techniques or very granular technical skill requirements</td>
<td>Highly Technical Specialists</td>
</tr>
</tbody>
</table>
# Specificity Levels

<table>
<thead>
<tr>
<th>I</th>
<th>CATEGORY</th>
<th>GRANULARITY</th>
<th>EXAMPLE CONTENT</th>
<th>EXAMPLE USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Broad category</td>
<td>OPM MOSAIC (Cybersecurity)</td>
<td>Background or Foundational Knowledge Requirements; Internships</td>
</tr>
<tr>
<td>II</td>
<td>SUBCATEGORY</td>
<td>Workrole, Functional Area, Major Duty</td>
<td>NICE Framework; DoD AT&amp;L; FAI FAC; CIP</td>
<td>Non-hands-on positions; Generalists</td>
</tr>
<tr>
<td>III</td>
<td>TYPE</td>
<td>Specific Technologies, Devices or Programming Languages</td>
<td>Vendor-specific certifications, specific programming languages, or technology-specific coursework</td>
<td>Hands-on positions</td>
</tr>
<tr>
<td>IV</td>
<td>SUBTYPE</td>
<td>Specific Techniques, Specialties, or Research Areas</td>
<td>Specific techniques or very granular technical skill requirements</td>
<td>Highly Technical Specialists</td>
</tr>
</tbody>
</table>
## Specificity Levels

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>GRANULARITY</th>
<th>EXAMPLE CONTENT</th>
<th>EXAMPLE USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I CATEGORY</td>
<td>Broad category</td>
<td>OPM MOSAIC (Cybersecurity)</td>
<td>Background or Foundational Knowledge Requirements; Internships</td>
</tr>
<tr>
<td>II SUBCATEGORY</td>
<td>Workrole, Functional Area, Major Duty</td>
<td>NICE Framework; DoD AT&amp;L; FAI FAC; CIP</td>
<td>Non-hands-on positions; Generalists</td>
</tr>
<tr>
<td>III TYPE</td>
<td>Specific Technologies, Devices or Programming Languages</td>
<td>Vendor-specific certifications, specific programming languages, or technology-specific coursework</td>
<td>Hands-on positions</td>
</tr>
<tr>
<td>IV SUBTYPE</td>
<td>Specific Techniques, Specialties, or Research Areas</td>
<td>Specific techniques or very granular technical skill requirements</td>
<td>Highly Technical Specialists</td>
</tr>
</tbody>
</table>
# Specificity Levels

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>GRANULARITY</th>
<th>EXAMPLE CONTENT</th>
<th>EXAMPLE USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Broad category</td>
<td>OPM MOSAIC (Cybersecurity)</td>
<td>Background or Foundational Knowledge Requirements; Internships</td>
</tr>
<tr>
<td>II</td>
<td>Workrole, Functional Area,</td>
<td>NICE Framework; DoD AT&amp;L; FAI FAC; CIP</td>
<td>Non-hands-on positions; Generalists</td>
</tr>
<tr>
<td>SUBCATEGORY</td>
<td>Major Duty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III</td>
<td>Specific Technologies,</td>
<td>Vendor-specific certifications, specific programming</td>
<td>Hands-on positions</td>
</tr>
<tr>
<td>TYPE</td>
<td>Devices or Programming</td>
<td>languages, or technology-specific coursework</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Languages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Specific Techniques,</td>
<td>Specific techniques or very granular technical skill</td>
<td>Highly Technical Specialists</td>
</tr>
<tr>
<td>SUBTYPE</td>
<td>Specialties, or Research</td>
<td>requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Areas</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Specificity Levels

<table>
<thead>
<tr>
<th></th>
<th>GRANULARITY</th>
<th>EXAMPLE CONTENT</th>
<th>EXAMPLE USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Broad category</td>
<td>OPM MOSAIC (Cybersecurity)</td>
<td>Background or Foundational Knowledge Requirements; Internships</td>
</tr>
<tr>
<td>II</td>
<td>Workrole, Functional Area, Major Duty</td>
<td>NICE Framework; DoD AT&amp;L; FAI FAC; CIP</td>
<td>Non-hands-on positions (Generalists)</td>
</tr>
<tr>
<td></td>
<td>Specific Technologies, Devices or Programming Languages</td>
<td>Ex. NICE Framework with Selective Drill-Down Vendor-specific certifications, specific programming languages, or technology-specific coursework</td>
<td>Hands-on positions</td>
</tr>
<tr>
<td>III</td>
<td>Specific Techniques, Specialties, or Research Areas</td>
<td>Specific techniques or very granular technical skill requirements</td>
<td>Highly Technical Specialists</td>
</tr>
</tbody>
</table>
## Specificity Levels

<table>
<thead>
<tr>
<th>I</th>
<th>CATEGORY</th>
<th>GRANULARITY</th>
<th>EXAMPLE CONTENT</th>
<th>EXAMPLE USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Broad category</td>
<td>OPM MOSAIC (Cybersecurity)</td>
<td>Background or Foundational Knowledge Requirements; Internships</td>
</tr>
<tr>
<td>II</td>
<td>SUBCATEGORY</td>
<td>Workrole, Functional Area, Major Duty</td>
<td>NICE Framework; DoD AT&amp;L; FAI FAC; CIP</td>
<td>Non-hands-on positions; Generalists</td>
</tr>
<tr>
<td>III</td>
<td>TYPE</td>
<td>Specific Technologies, Devices or Programming Languages</td>
<td>Vendor-specific certifications, specific programming languages, or technology-specific coursework</td>
<td>Hands-on positions</td>
</tr>
<tr>
<td>IV</td>
<td>SUBTYPE</td>
<td>Specific Techniques, Specialties, or Research Areas</td>
<td>Specific techniques or very granular technical skill requirements</td>
<td>Highly Technical Specialists</td>
</tr>
</tbody>
</table>
Case Study: Security Programmer

LEVEL I

CATEGORY-LEVEL COMPETENCIES & KSA’s

OPM MOSAIC-Level Example (Multipurpose Occupational Systems Analysis Inventory - Close-Ended)

- Computer Languages - Knowledge of computer languages and their applications to enable a system to perform specific functions.
- Information Assurance - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
- Information Systems Security Certification - Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.
- Information Systems/Network Security - Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

SOURCE: https://www.chcoc.gov/content/competency-model-cybersecurity

Case Study: Security Programmer

LEVEL II

CATEGORY-LEVEL COMPETENCIES & KSA’s

OPM MOSAIC-Level Example (Multipurpose Occupational Systems Analysis Inventory - Close-Ended)

- **Computer Languages** - Knowledge of computer languages and their applications to enable a system to perform specific functions.

- **Information Assurance** - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.

- **Information Systems Security Certification** - Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.

- **Information Systems/Network Security** - Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

SOURCE: [https://www.chcoc.gov/content/competency-model-cybersecurity](https://www.chcoc.gov/content/competency-model-cybersecurity)

Case Study: Security Programmer (Continued)

LEVEL II

SUBCATEGORY-LEVEL COMPETENCIES & KSA’s

Example ORGANIZED BY MAJOR DUTIES OR WORKROLES

PROACTIVE:

- **Secure Coding** – skills describing someone who develops secure code. Will be specialized in one or more programming languages. This person is a developer.

- **Code Reviewing** - skills describing someone who reviews code for security flaws. Will be specialized in one or more programming languages. This person is NOT a developer, but more along the lines of a Vulnerability Analyst.

CONTINUOUS:

- **Code Validation & Integrity Checking** - skills describing the process of digitally signing code, then validating authenticity throughout the lifecycle (including patching and updating). May not actually be a programmer or understand code at all. Generally may need some knowledge of cryptographic hashes, checksums, operational update processes, etc.

REACTIVE:

- **Malware Analysis** - skills describing someone who can analyze code injected into systems, hardware, software, etc. Generally must have some knowledge of Assembler and at least one other programming language.

- **Forensics Analyst Analysis** - skills describing someone who can harvest malware

- **Law Enforcement Forensics Analysis** - able to testify in court or prepare evidence sufficiently for court about harvested malware.
PROACTIVE:

- **Secure Coding** – skills describing someone who develops secure code. Will be specialized in one or more programming languages. This person is a developer.

- **Code Reviewing** - skills describing someone who reviews code for security flaws. Will be specialized in one or more programming languages. This person is NOT a developer, but more along the lines of a Vulnerability Analyst.

CONTINUOUS:

- **Code Validation & Integrity Checking** - skills describing the process of digitally signing code, then validating authenticity throughout the lifecycle (including patching and updating). May not actually be a programmer or understand code at all. Generally may need some knowledge of cryptographic hashes, checksums, operational update processes, etc.

REACTIVE:

- **Malware Analysis** - skills describing someone who can analyze code injected into systems, hardware, software, etc. Generally must have some knowledge of Assembler and at least one other programming language.

- **Forensics Analyst Analysis** - skills describing someone who can harvest malware

- **Law Enforcement Forensics Analysis** - able to testify in court or prepare evidence sufficiently for court about harvested malware.
<table>
<thead>
<tr>
<th>Ex: Specific Technology, Programming Language, Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEVEL III</strong></td>
</tr>
<tr>
<td>Case Study: Security Programmer</td>
</tr>
<tr>
<td><strong>TYPE-LEVEL COMPETENCIES &amp; KSA’s – Ex:</strong></td>
</tr>
<tr>
<td><strong>SPECIALIZED TECHNOLOGY, PROGRAMMING LANGUAGE, DEVICE</strong></td>
</tr>
<tr>
<td><strong>Ex:</strong> Security Engineering</td>
</tr>
<tr>
<td><strong>Technology:</strong></td>
</tr>
<tr>
<td><strong>Programming Language:</strong></td>
</tr>
<tr>
<td><strong>Device:</strong></td>
</tr>
</tbody>
</table>

### Table of Specific Technologies, Programming Languages, and Devices

<table>
<thead>
<tr>
<th>Technology</th>
<th>Programming Languages</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Engineering</td>
<td>Security</td>
<td></td>
</tr>
</tbody>
</table>
LEVEL III

Case Study: Security Programmer

TYPE-LEVEL COMPETENCIES & KSA's – Ex. SPECIFIC TECHNOLOGY, PROGRAMMING LANGUAGE, DEVICE

Which of the 400’ish Programming Languages do you need?

60
Case Study: Security Programmer (Continued)

LEVEL I

CATEGORY-LEVEL COMPETENCIES & KSA’s

OPM MOSAIC-Level Example (Multipurpose Occupational Systems Analysis Inventory - Close-Ended)

- **Computer Languages** - Knowledge of computer languages and their applications to enable a system to perform specific functions.

- **Information Assurance** - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.

- **Information Systems Security Certification** - Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.

- **Information Systems/Network Security** - Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

SOURCE: [https://www.chcoc.gov/content/competency-model-cybersecurity](https://www.chcoc.gov/content/competency-model-cybersecurity)

LEVEL I

CATEGORY-LEVEL COMPETENCIES & KSA’s

OPM MOSAIC-Level Example (Multipurpose Occupational Systems Analysis Inventory - Close-Ended)

- **Computer Languages** - Knowledge of computer languages and their applications to enable a system to perform specific functions.

- **Information Assurance** - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.

- **Information Systems Security Certification** - Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.

- **Information Systems/Network Security** - Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

SOURCE: [https://www.chcoc.gov/content/competency-model-cybersecurity](https://www.chcoc.gov/content/competency-model-cybersecurity)

<table>
<thead>
<tr>
<th>Level II to III</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Programmer</strong></td>
</tr>
<tr>
<td><strong>SUBCATEGORY-LEVEL COMPETENCIES &amp; KSAs</strong> – Ex. ORGANIZED BY MAJOR DUTIES OR WORKROLES</td>
</tr>
</tbody>
</table>

**Case Study: Security Programmer**
<table>
<thead>
<tr>
<th>Job Title</th>
<th>Subcategory-Level Competencies &amp; KSA's</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Case Study: Security Programmer</strong></td>
<td><strong>Ex. ORGANIZED BY MAJOR DUTIES OR WORKROLES</strong></td>
</tr>
<tr>
<td><strong>LEVEL II to III</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Which of the 360’ish Cyber-related Functions or Job Titles are involved?</strong></td>
<td></td>
</tr>
</tbody>
</table>
OMG.
OMG..
I’M NOT DOING THAT..!!
DHS PushButtonPD™ NICE Framework Demonstration
Yes.. much better.. 😊
Filtering the Pandora’s Box

• **What is a good Task to include?**
  - If the employee does not do it, will you go to HR about it?
  - Is it reasonable that a single person can do all the tasks?
  - Does this (unintentionally) overlap or duplicate with tasks performed by others?
  - Is it well-defined and accurately reflect the Major Duties (vs vague and generic)?

• **What is a good Competency or KSA to include?**
  - Is it a *need* (not a *want*)?
  - Is it *measurable*? Is it (in some form or another) on their resume or can you interview / test on it – not (a) something you will on-the-job train them later to do; or (b) too vague and opinionated?
  - Are there equivalent or suitable alternatives that are just as good (*or* versus *and*)?
Continuing to Filter the Pandora’s Box

“Special Qualification Requirements - a statement of any valid knowledge, skill, education, certification, etc., required by the position if it is not readily apparent from reading the description, such as level of typing skill, foreign language proficiency, or licensure.”


• What is a good Competency or KSA to use as a Special Qualification or a Selective Placement Factor?
  • Is it sufficiently defined to easily pick it out when resume screening? If not, are you able to test it in an interview or phone screen?
  • Do you want to eliminate and screen out candidates without it on their resume? (e.g. a minimum threshold to achieve)
  • Is it truly special (versus commonplace)?
Q & A
Live Demo

DHS PushButtonPD™ NICE Framework Demonstration
Questions

Writing Cybersecurity Job Descriptions for the Greatest Impact
Helpful Resources

NIST NICE, NICE.nist@nist.gov, https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity

DHS NPPD NICCS Website (Workforce Development page), https://niccs.us-cert.gov/workforce-development, NICCS@hq.dhs.gov

The NICCS Training Catalog – more than 3,000 cybersecurity courses (including certification prep courses) already aligned to the NICE Framework

The Workforce Development Toolkit – a gateway of sorts to many other white papers, best practices, and templates organizations can use for workforce planning and other development activities https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit


Demo
We're looking for personable, adaptable, skilled and experienced engineers to join our team. You like a lot of variety in your job, love tackling the hard technology problems that scale introduces, are not fazed by change, and can both think strategically about the future as well as dig deep into problems affecting our users and business today.
We're looking for personable, adaptable, skilled and experienced engineers to join our team. You like a lot of variety in your job, love tackling the hard technology problems that scale introduces, are not fazed by change, and can both think strategically about the future as well as dig deep into problems affecting our users and business today.
We're looking for personable, adaptable, skilled and experienced engineers to join our team. You like a lot of variety in your job, love tackling the hard technology problems that scale introduces, are not fazed by change, and can both think strategically about the future as well as dig deep into problems affecting our users and business today.
Before RecruitHer:

We're looking for personable, adaptable, skilled and experienced engineers to join our team. You like a lot of variety in your job, love tackling the hard technology problems that scale introduces, are not fazed by change, and can both think strategically about the future as well as dig deep into problems affecting our users and business today.
After RecruitHer:

We're looking for personable, adaptable, skilled and experienced engineers to join our team. You like a lot of variety in your job, **love learning about and solving** the hard technology problems that scale introduces, are not fazed by change, and can both **think creatively** about the future as well as dig deep into problems affecting our users and business today.
RecruitHer

We're looking for personable, adaptable, skilled and experienced engineers to join our team. You like a lot of variety in your job, love tackling the hard technology problems that scale introduces, are not fazed by change, and can both think strategically about the future as well as dig deep into problems affecting our users and business today.

think strategically

<table>
<thead>
<tr>
<th>Think strategically - Strongly Male</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendation</strong></td>
<td><strong>Gender Leaning</strong></td>
<td><strong>Similarity Score</strong></td>
</tr>
<tr>
<td>Innovative thinker</td>
<td>Male</td>
<td>77.2%</td>
</tr>
<tr>
<td>Growth mindset</td>
<td>Strongly Male</td>
<td>74.5%</td>
</tr>
<tr>
<td>Organisational managerial</td>
<td>Male</td>
<td>73.3%</td>
</tr>
<tr>
<td>Visionary leader</td>
<td>Strongly Male</td>
<td>73.3%</td>
</tr>
<tr>
<td>Think critically</td>
<td>Strongly Male</td>
<td>73.2%</td>
</tr>
<tr>
<td>Entrepreneurial attitude</td>
<td>Male</td>
<td>72.9%</td>
</tr>
<tr>
<td>Strategically important</td>
<td>Male</td>
<td>72.8%</td>
</tr>
<tr>
<td>Strategist who</td>
<td>Strongly Male</td>
<td>69.2%</td>
</tr>
<tr>
<td>Ability improvise</td>
<td>Male</td>
<td>68.6%</td>
</tr>
<tr>
<td>Visionary</td>
<td>Male</td>
<td>68.3%</td>
</tr>
</tbody>
</table>
Q & A
Thank You for Joining Us!

**Upcoming Webinar:** Development of Soft Skills That Are In Demand by Cybersecurity Employers

**When:** Wednesday, February 21, 2018 at 2:00pm EST

Visit the event website [here](https://nist-nice.adobeconnect.com/webinar-february2018/event/registration.html) for more information.


[nist.gov/nice/webinars](https://nist.gov/nice/webinars)