

MODERNIZING DOW HIRING

A SKILLS-BASED APPROACH TO BUILDING OUR CYBER WORKFORCE

Matt Isnor

Workforce Innovation Directorate

DoW CIO | March 2026





The Challenge & Our Solution

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

THE CHALLENGE: A CRITICAL GAP IN OUR CYBER DEFENSES

- The Department of Defense has an urgent need for cybersecurity experts to counter evolving threats.
- We have over 7,600 unfilled cyber positions.
- Traditional hiring methods are slow and struggle to identify the right talent quickly.

THE SOLUTION: SKILLS BASED HIRING

- **Why Skilled-based Assessments:** A modern approach, aligned with White House Executive Orders 13932 & 14170, that focuses on what candidates can do, not just their resume.
- **Value:**
 - ✓ *Fills Critical Roles Faster*
 - ✓ *Hires the Most Qualified Talent*
 - ✓ *Expands the Talent Pool*
 - ✓ *Ensures Objective, Data-Driven Decisions*



What is Skills-Based Hiring?

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

It's a simple and powerful idea: *Prove your skills through performance*

The screenshot shows a computer interface for a skills-based hiring challenge. On the left, a file explorer window displays a folder named 'USB_Image' containing a file 'deps_installer.hta'. A central window shows a 'Detection Ratio' chart with a red circle indicating '13/76'. Below the chart, a table lists detection results: 13 MALICIOUS, 0 SUSPICIOUS, 48 UNDETECTED, and 0 HARMLESS. At the bottom, 'File Information' is shown for 'deps_installer.hta', including file type (HTML), size (631 bytes), and MD5 hash. On the right, a submission form asks questions about the file's maliciousness and provides a 'Submit' button. A 'TIME REMAINING: 27 MINUTES' timer is visible at the top right.

WHAT IT IS:

- ✓ A hiring method that uses practical, hands-on challenges to measure a candidate's actual abilities.

HOW IT IMPROVES THE PROCESS:

- ✓ We use skills assessments during the application window to quickly identify top candidates, which is especially effective for technical roles with high applicant volumes.

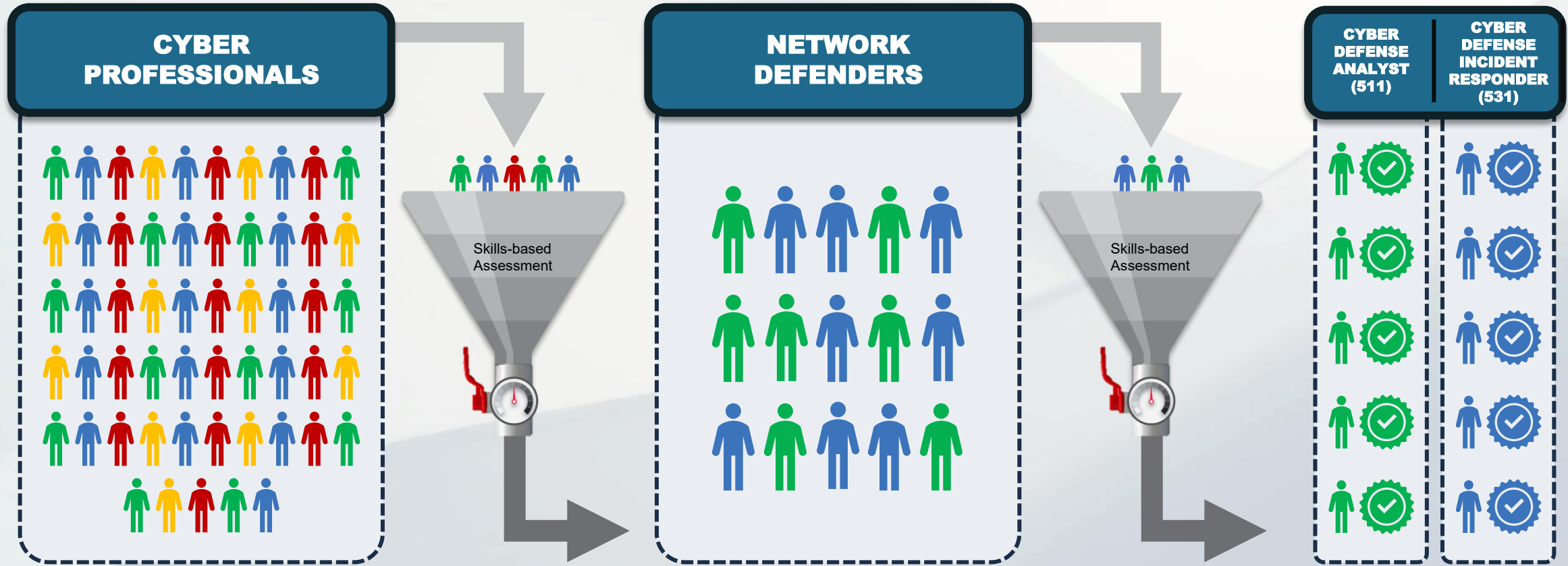
THE GOAL:

- ✓ To hire individuals who are ready to perform in critical roles from day one, based on objective proof of their skills.



Skills-Based Hiring Assessments

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010





“Real World” Skill-based Assessments

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

- **Validated Skill-Based Assessments:** Rigorously validated to confirm their effectiveness in measuring technical skills.
- **DCWF Work Role Alignment:** Each assessment is directly mapped to the specific cyber work roles outlined in the DCWF.
- **Customizable Cyber Range:** We utilize a proprietary, in-house developed cyber range that can be highly customized to simulate various operational environments.
- **Real-World KSAT Evaluation:** The platform is designed to evaluate a candidate's technical Knowledge, Skills, Abilities, and Tasks (KSATs) through practical, real-world scenarios.

TIME REMAINING: 29 MINUTES End Challenge

Source IP Address(es) of Malicious Traffic:
Each IP address should be a separate entry. Click the Add Entry button to add as many entries as necessary.

102.129.235.127
192.168.0.1
[Add Entry](#)

Destination IP Address(es) of Malicious Traffic:
Each IP address should be a separate entry. Click the Add Entry button to add as many entries as necessary.

34.169.128.124
[Add Entry](#)

Time of First Authentication Attempt:
Use the format HH:MM:SS in 24 hour format. Do not round, provide fractional seconds, or convert to UTC.

21:34:56

Were Any Credentials Compromised?
Yes No

Compromised User Account(s):
Each user account should be a separate entry. Click the Add Entry button to add as many entries as necessary.

userone
[Add Entry](#)

Time of First Successful Authentication:
Use the format HH:MM:SS in 24 hour format. Do not round, provide fractional seconds, or convert to UTC.

21:34:56

Time of Last Authentication Attempt:
Use the format HH:MM:SS in 24 hour format. Do not round, provide fractional seconds, or convert to UTC.

21:34:56

Submit

T
L
A
S
S
K

Case Report Submitted



Our Roadmap: From Pilot to Enterprise Capability

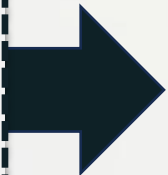
01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

From Concept to Capability

PILOT AND VALIDATE

(Now – Q2 FY26)

- Execute live pilot for Cyber Defender roles.
- Refine assessment framework.
- Validate with OPM and other partners.



EXPAND & IMPLEMENT

(FY26 -27)

- Host first skills-based hiring events.
- Expand to 10% of all open cyber jobs.
- Develop assessments for more work roles.



SCALE TO ENTERPRISE

(FY27 and Beyond)

- Integrate with CYBERCOM force generation.
- Publish DoW-wide adoption playbook.
- Become the standard for Cyber Workforce hiring.