



July 2023

CYBERSECURITY WORKFORCE

National Initiative Needs to Better Assess Its Performance

GAO Highlights

Highlights of [GAO-23-105945](#), a report to congressional requesters

Why GAO Did This Study

A well-trained cybersecurity workforce is essential for government functioning. To bolster that workforce, NIST has developed the National Initiative for Cybersecurity Education (NICE). This program's mission is to foster more education and training through collaborative partnerships with private industry, academia, and government agencies.

GAO was asked to review the progress the NICE program is making against its stated goals and objectives. This report examines (1) the actions NIST has taken through the NICE program to strengthen the cybersecurity workforce and (2) the extent to which NIST established a process to assess the program's performance.

GAO analyzed documents related to NIST's program performance assessments and compared these to selected key performance practices identified in legislation and prior GAO work. GAO also conducted focus group interviews with active program participants about their experiences. Additionally, GAO interviewed NIST officials responsible for the program.

What GAO Recommends

GAO is making eight recommendations to NIST to fully develop goals and performance measures, assess the program's environment and identify strategies, track reliable information and report to stakeholders on results, and use data to assess progress and identify improvement opportunities. The Department of Commerce agreed with the recommendations and suggested wording revisions, which GAO incorporated as appropriate.

View [GAO-23-105945](#). For more information, contact David B. Hinchman at (214) 777-5719, or hinchmand@gao.gov.

July 2023

CYBERSECURITY WORKFORCE

National Initiative Needs to Better Assess Its Performance

What GAO Found

The National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) program has taken steps to strengthen the cybersecurity workforce. For example:

- The program established an inventory or "framework" of necessary skills and work roles associated with cybersecurity and expanded it with stakeholder input.
- The program formed public and private collaborations to connect the cybersecurity community and promote cybersecurity training and education. This included working groups and communities of interest run in part by volunteers. These groups created projects based on one of the NICE program's strategic goals or the needs of a specific cybersecurity community.
- The program holds periodic webinars, quarterly forums, and multiple annual conferences to share information on cybersecurity issues.

In focus group discussions with program volunteers from industry, academia, and government, participants cited what they regarded as successes, including robust community benefits. However, some participants noted challenges with the program, such as an unclear scope.

NIST's process for assessing the NICE program included fully implementing the practice of involving stakeholders. However, other key practices for establishing a program-level performance process were not fully implemented. Specifically, of nine selected key performance assessment practices, NIST fully implemented one, partially implemented five, and did not implement three (see figure).

National Institute of Standards and Technology (NIST) Implementation of Selected Key Practices for Establishing a Program Performance Process

Practice	Implementation
Develop measurable outcome-based goals	Partial implementation
Assess the program environment	
Identify strategies and resources	
Involve stakeholders	Full implementation
Develop performance measures	No implementation
Track information that is timely/accurate/useful	
Regularly communicate progress to stakeholders	
Use data to assess progress towards goals and identify any gaps	
Identify opportunities to improve program management and results	

Source: GAO analysis of NIST information. | GAO-23-105945

For example, NIST did not develop performance measures for the program. According to program officials, they relied on the program's volunteer working groups to develop such measures. However, the variability in skills and approaches of the volunteers made it too difficult to accomplish. As a result, NIST was unable to demonstrate program progress. Without reliable data to manage the NICE program's performance, NIST is not in a position to effectively and efficiently identify obstacles or opportunities to sustain and improve the initiative.

Contents

Letter		1
	Background	4
	NIST Took Actions through the NICE Program to Strengthen the Cybersecurity Workforce; Selected Participants Noted Successes and Challenges	11
	NIST Partially Implemented Most Key Practices to Assess Program Performance	31
	Conclusions	36
	Recommendations for Executive Action	36
	Agency Comments and Our Evaluation	37
Appendix I	Objectives, Scope, and Methodology	39
Appendix II	NICE Program Successes and Challenges Identified by Focus Groups	43
Appendix III	Comments from the Department of Commerce	48
Appendix IV	GAO Contact and Staff Acknowledgments	52
Tables		
	Table 1: Selected Program Performance Process Key Practices	10
	Table 2: National Initiative for Cybersecurity Education (NICE) Events That the Program Hosts or Coordinates	18
	Table 3: NIST's Implementation of Selected Key Performance Assessment Practices for Defining Goals for the NICE Program	31
	Table 4: NIST's Implementation of Selected Key Performance Assessment Practices for Collecting Performance Data for the NICE Program	33
	Table 5: NIST's Implementation of Selected Key Practices for Using Performance Data for the NICE Program	35
	Table 6: National Initiative for Cybersecurity Education (NICE) Program Successes Identified by Focus Groups	43

Table 7: National Initiative for Cybersecurity Education (NICE) Program Challenges Identified by Focus Groups	44
--	----

Figures

Figure 1: National Institute of Standards and Technology Organization Chart, Including the NICE Program	5
Figure 2: National Initiative for Cybersecurity Education (NICE) Interagency Coordinating Council, Community Coordinating Council, Working Groups, and Communities of Interest as of May 2023	13
Figure 3: National Initiative for Cybersecurity Education (NICE) Working Groups and Communities of Interest with the NICE Program’s Five Strategic Goals as of May 2023	17
Figure 4: First and Subsequent Occurrences of the Events the National Initiative for Cybersecurity Education (NICE) Program Hosts or Coordinates, August 2010-June 2023	19
Figure 5: National Initiative for Cybersecurity Education (NICE) Program Successes Identified by Focus Groups of NICE Volunteers	21
Figure 6: National Initiative for Cybersecurity Education (NICE) Program Challenges Identified by Focus Groups of NICE Volunteers	25

Abbreviations

COVID-19	coronavirus disease 2019
FISSEA	Federal Information Security Educators
GPRA	Government Performance and Results Act
IT	information technology
K12	kindergarten through grade 12
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



July 27, 2023

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Kyrsten Sinema
Chair
Subcommittee on Government Operations and Border Management
Committee on Homeland Security and Governmental Affairs
United States Senate

A resilient, skilled, and dedicated cybersecurity workforce is essential to protecting federal IT systems as well as enabling the government’s day-to-day functions.¹ Building and maintaining the IT workforce by addressing mission-critical skills gaps is one of the federal government’s most important challenges as well as a national security priority. The ability to secure federal IT systems depends on the knowledge, skills, and abilities of the federal and contractor cybersecurity workforce that uses, implements, secures, and maintains these systems. Nevertheless, the Office of Management and Budget and our prior reports have pointed out that the federal government faces a persistent shortage of cybersecurity and IT professionals.²

¹For the purposes of this report, we will refer to “cyber” and “cybersecurity” as “cybersecurity” unless otherwise stated.

²Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (July 12, 2016); and GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021).

We and other organizations have previously reported that agencies faced challenges ensuring they have an effective cybersecurity workforce.³ In 1997, we designated the security of federal IT systems as a government-wide high-risk area and noted the shortage of information security personnel with the technical expertise required to manage controls in these systems.⁴ In 2001, we added strategic human capital management to our High-Risk List.⁵ In our 2023 update to the High-Risk List, we reported that continuing efforts of the federal government and Office of Personnel Management are needed to address mission-critical, government-wide skills gaps in fields such as cybersecurity.⁶

To help agencies in their cybersecurity workforce planning efforts, the National Institute of Standards and Technology (NIST) has been involved in developing standards and initiatives related to cybersecurity priority areas such as education and workforce. One of these initiatives is the National Initiative for Cybersecurity Education (NICE) program, which is a partnership among the industry, academia, and government sectors to help strengthen cybersecurity education, training, and workforce development.

You asked us to review the progress of the NICE program against its stated goals and objectives. This report examines (1) the actions NIST has taken through the NICE program to strengthen the cybersecurity workforce and (2) the extent to which NIST established a process to assess the program's performance.

³GAO, *Information Technology: Biannual Scorecards Have Evolved and Served As Effective Oversight Tools*, [GAO-22-105659](#) (Washington, D.C.: Jan. 20, 2022); *Federal Management: Selected Reforms Could Be Strengthened by Following Additional Planning, Communication, and Leadership Practices*, [GAO-20-322](#) (Washington, D.C.: Apr. 23, 2020); National Academy of Public Administration, *A Call to Action—The Federal Government's Role in Building a Cybersecurity Workforce for the Nation* (Washington D.C.: January 2022); and Cyberspace Solarium Commission, *Workforce Development Agenda for the National Cyber Director* (June 2022).

⁴GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: Feb. 1, 1997).

⁵Strategic human capital management refers to the talent management activities, such as robust workforce planning and training, that agencies conduct to address challenges in the federal workforce, including skills gaps. See GAO, *Human Capital: Meeting the Government-wide High-Risk Challenge*, [GAO-01-357T](#) (Washington, D.C.: Feb. 1, 2001).

⁶GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, [GAO-23-106203](#) (Washington, D.C.: Apr. 20, 2023).

To answer our objectives, we reviewed and analyzed key documents—including NIST meeting agendas, meeting minutes, community group charters, and program performance information. Additionally, we conducted six focus groups featuring NICE community volunteers from across industry, academia, and government sectors to better understand the successes and challenges the program faces. Within each of these three sectors, we organized active program volunteer members into two subcategories: leadership and nonleadership. We identified leadership members as those who held or had previously held a leadership role—such as being a co-chair of a working group or community of interest. We identified members as nonleadership if they had not held such a role. We used a randomization formula within each of the six groups to determine the order in which we reached out to volunteers to participate in focus group interviews. With all six focus groups, we discussed the volunteers’ experience as members of a NICE community group. Though random selection was used to mitigate selection bias, the information gathered from the interviews and focus groups is not generalizable and is meant to provide illustrative examples.

To determine the extent to which NIST established a performance assessment process for the NICE program, we compared the agency’s practices to selected key practices for assessing program performance management.⁷ Additionally, we interviewed NIST officials from the NICE program office regarding information related to both objectives. For more information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from May 2022 to July 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings.

⁷Selected key practices in program performance management came from the Government Performance and Results Act of 1993 (GPRA), the GPRA Modernization Act of 2010, and GAO, *Veterans Justice Outreach Program: VA Could Improve Management by Establishing Performance Measures and Fully Assessing Risks*, [GAO-16-393](#) (Washington, D.C.: Apr. 28, 2016); *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, [GAO-05-927](#) (Washington, D.C.: Sept. 9, 2005); and *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1, 1996).

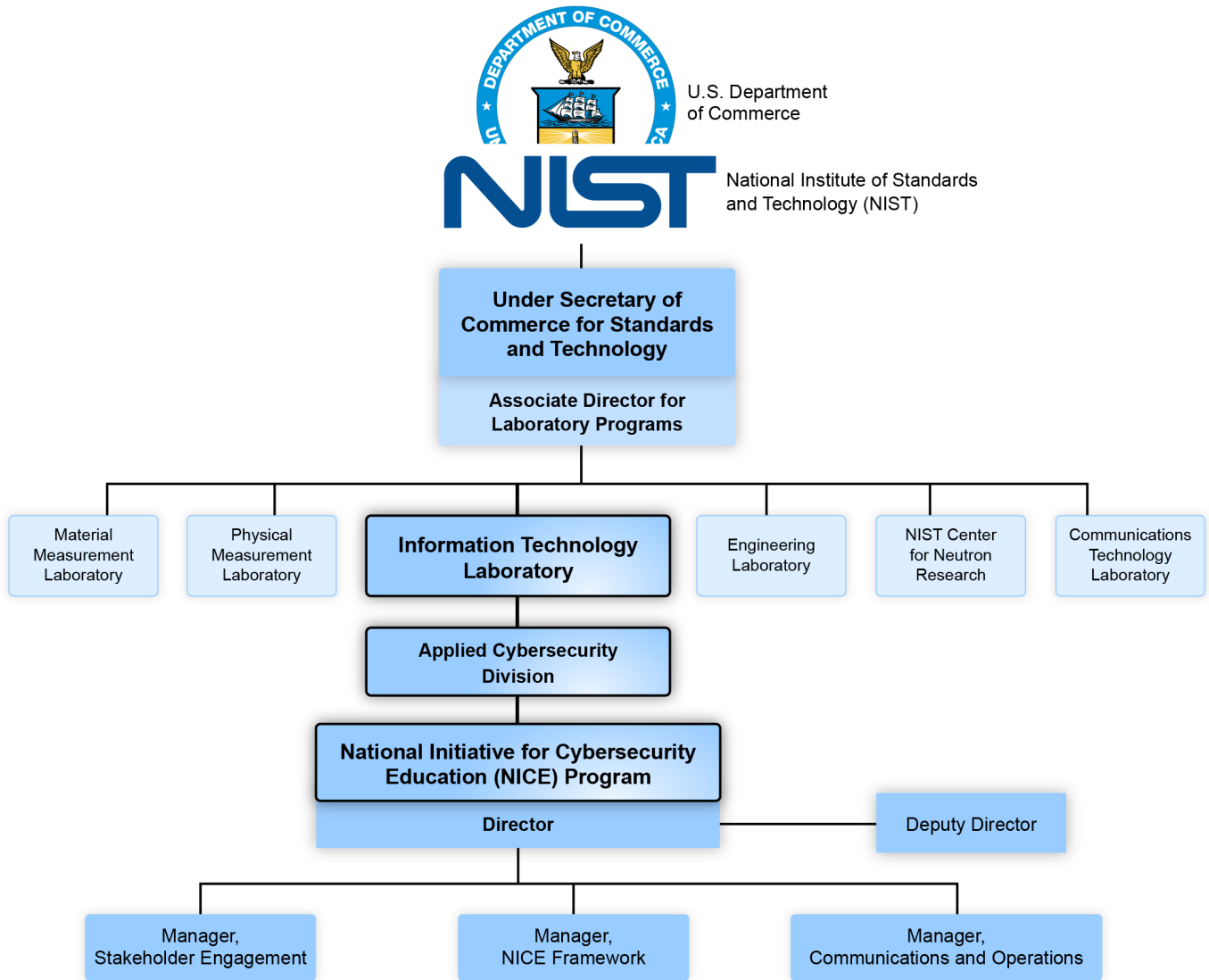
Background

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.⁸ NIST develops cybersecurity standards, guidelines, best practices, and other resources driven by both federal mandates as well as industry and public needs. The Under Secretary of Commerce for Standards and Technology serves as Director of NIST, the agency coordinating the NICE program partnership among the industry, academia, and government sectors.

The NICE program operates within the Information Technology Laboratory, one of NIST's six research laboratories. NIST's Associate Director for Laboratory Programs leads all six laboratory programs and, among other responsibilities, provides direction, operational guidance, and program and budget development leadership for these scientific and technical laboratory programs. The Information Technology Laboratory has six divisions, two of which focus on cybersecurity: the Computer Security and Applied Cybersecurity divisions. The NICE program office operates within the Applied Cybersecurity division. Figure 1 depicts how NIST's laboratories and divisions are organized and shows where the program fits in this structure.

⁸National Institute of Standards and Technology (NIST), "About NIST," accessed May 19, 2023, <https://www.nist.gov/about-nist>.

Figure 1: National Institute of Standards and Technology Organization Chart, Including the NICE Program



Sources: GAO analysis of NIST information; Department of Commerce (logos). | GAO-23-105945

Development of the NICE Program and Its Mission

According to NIST officials, the NICE program originated with Initiative 8 of the 2008 Comprehensive National Cybersecurity Initiative, which called

for expanding cybersecurity education efforts to the national level.⁹ Originally, NIST served as the program lead, while six federal agencies initially led the four components comprising the program.¹⁰ The Cybersecurity Enhancement Act of 2014 authorized NIST to create a cybersecurity workforce program to coordinate with industry, academia, and government.¹¹

The NICE program's mission is to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.¹² To address this mission, the program coordinates with industry, academic, and government partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision for the cybersecurity workforce. These coordination efforts work to increase the number of skilled cybersecurity professionals helping to keep our nation secure.¹³

In 2020, the NICE program office announced a strategic plan for calendar years 2021 through 2025. The plan was developed with assistance from NICE partners in the industry, academia, and government sectors. The overall intent of the strategic plan was to promote a national conversation

⁹National Security Presidential Directive 54/ Homeland Security Presidential Directive 23, Initiative 8 (Washington, D.C.: Jan. 8, 2008).

¹⁰The 2012 NICE Strategic Plan laid out four NICE program components. The Department of Homeland Security (DHS) led Component 1: National Cybersecurity Awareness; the National Science Foundation and the Department of Education led Component 2: Formal Cybersecurity Education; the Department of Homeland Security and the Office of Personnel Management led Component 3: Cybersecurity Workforce Structure; and the Department of Homeland Security, the Department of Defense, and the Office of the Director of National Intelligence led Component 4: Cybersecurity Workforce Training and Professional Development.

¹¹Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, title IV, § 401, 128 Stat. 2971, 2985-86 (2014), codified as amended at 15 U.S.C. § 7443.

¹²National Institute of Standards and Technology (NIST), "National Initiative for Cybersecurity Education (NICE): About," accessed May 19, 2023, <https://www.nist.gov/itl/applied-cybersecurity/nice/about>.

¹³NIST program officials defined "industry" as private sector companies, trade associations, and training and certification providers (who are for-profit or of a commercial nature). The program defines "academia" as kindergarten through grade 12 (K12) education and post-secondary education institutions, associations, and nonprofits that serve the education sector. The government sector, as defined by the program, includes federal, tribal, state, local, and territorial governments.

and guide actions on addressing the critical shortage of a skilled cybersecurity workforce. The program's five strategic goals are the following:

1. Promote the discovery of cybersecurity careers and multiple pathways
2. Transform learning to build and sustain a diverse and skilled workforce
3. Modernize the talent management process to address cybersecurity skills gaps
4. Expand the use of the *Workforce Framework for Cybersecurity* (the framework)¹⁴
5. Drive research on effective practices for cybersecurity workforce development

NIST officials provided information on the NICE program's budget, administrative staffing, and process for coordinating with stakeholders as of May 2023. Specifically, the program has a \$4 million annual budget and has a staff comprised of eight full-time equivalent employees and part-time contractors who work on a task-related basis. The Director of NICE has a policy, management, and hiring role. The Deputy Director also serves as the Manager for Stakeholder Engagement, coordinating the work of staff leads for academic engagement, industry engagement, government engagement, and international engagement. The stakeholder engagement team coordinates weekly as part of NICE staff meetings and holds quarterly strategy sessions to refine practices and coordinate implementation. Additionally, the NICE program has an office manager to conduct administrative work such as coordinating travel, managing office supplies, and other administrative tasks.

NICE Workforce Framework for Cybersecurity

To help the federal government better understand the breadth of cybersecurity work, NIST developed the *Workforce Framework for Cybersecurity*, which organizes a consistent reference taxonomy around cybersecurity work and the individuals who carry it out. This framework describes and shares information about cybersecurity work by helping identify, recruit, develop, and retain cybersecurity talent. It accomplishes this through task, knowledge, and skill statements, otherwise called

¹⁴As described in the following section, the framework is a reference published by the NICE program that provides a common language for describing the tasks, knowledge, and skills needed for individuals and teams to perform cybersecurity work.

“building blocks.” The framework is intended to be applied in the public, private, and academic sectors.

The concept for the framework began before the establishment of the NICE program in 2010 and grew out of the recognition that the cybersecurity workforce had not been defined and assessed. In 2007, the Department of Homeland Security formed the IT Security Essential Body of Knowledge, which is a competency and functional baseline of essential knowledge and skills for IT security workforce development. In 2008, the Federal Chief Information Officers Council started to build on this and provided a standard reference tool to understand the cybersecurity roles within the federal government. The NICE program published the first version of the framework in 2012. The framework underwent multiple revisions that expanded its scope to allow both the public and private sectors to use it as a reference tool. The program published the fourth and current version of the framework in November 2020.¹⁵

The framework introduced work roles as detailed descriptions of the roles and responsibilities of IT, cybersecurity, and cyber-related job functions. Work roles contain a collection of tasks that comprise the work to be done within that role. Tasks, in turn, are associated with

- **skill statements**, which describe what a learner can do (e.g., “skills in recognizing the alerts of an intrusion detection system”), and
- **knowledge statements**, which lay out the concepts a learner may need to understand or the expertise needed to complete a task (e.g., “knowledge of cyberspace threats and vulnerabilities”).

According to the framework, multiple skill or knowledge statements may be needed to complete a task, and a skill or knowledge statement may be associated with multiple tasks.

Selected Key Practices for Program Performance Processes

A performance assessment process documented in a robust performance plan is necessary for results-based performance management and assessment of federal programs.¹⁶ Federal agencies that measure progress toward and assess achievement of their strategic goals using

¹⁵National Institute of Standards and Technology, *Workforce Framework for Cybersecurity (NICE Framework)*, Special Publication 800-181 revision 1 (Gaithersburg, MD: November 2020).

¹⁶A performance plan is a document in which program management can measure progress toward the achievement of both the annual goals linked to long-term and strategic plan goals.

performance measures demonstrate accountability and inform taxpayers on what the government provides in return for their tax dollars. Using performance measures can help federal programs such as NICE identify performance gaps and improve program processes. This could help program managers better understand costs associated with program performance and how to improve or sustain this performance.

Our prior work has found that choosing performance measures that tell each organizational level how well it is achieving its goals poses an especially difficult challenge for federal managers of research programs. This is due, in part, to difficulties establishing the link between federal efforts and desired outcomes, which may not be apparent for years.¹⁷ Nonetheless, producing qualitative or quantitative performance measures for agency goals and objectives allows managers to assess progress and, if necessary, make changes. In circumstances where objectives cannot be easily expressed through quantitative measures, managers may use qualitative measures. For example, a program that has not yet designed a formal survey on its publications could conduct an analysis of individual feedback, such as written comments.

To improve the efficiency and effectiveness of federal programs, Congress and the President enacted the Government Performance and Results Act of 1993 (GPRA)¹⁸ and significantly amended and expanded requirements through the GPRA Modernization Act of 2010.¹⁹ Broadly, GPRA, as amended, contains a number of requirements that align with a performance assessment model. Among other things, this legislation requires agencies to

- develop strategic plans containing mission statements and outcome-related strategic goals,
- develop annual performance plans with performance goals and indicators to measure performance, and
- prepare annual reports on the results achieved toward performance goals.

¹⁷See, for example, GAO, *Department of Energy: Improved Performance Planning Could Strengthen Technology Transfer*, [GAO-21-202](#) (Washington, D.C.: Feb. 1, 2021), and [GAO/GGD-96-118](#).

¹⁸Pub. L. No. 103-62, 107 Stat. 285 (1993).

¹⁹Pub. L. No. 111-352, 124 Stat. 3866 (2011).

While GPRA, as amended, applies at the department or agency level, prior GAO work has found that these requirements on results-based performance management can serve as key practices for program-level performance assessment.²⁰

The performance assessment process can be expressed in three steps: (1) define goals, (2) collect data, and (3) use data. Within these three areas are nine selected key performance practices from GPRA and our past work that are central to effectively assessing program management (see table 1).

Table 1: Selected Program Performance Process Key Practices

Step for performance assessment	Performance assessment key practice	Description of related legal requirements that can serve as performance assessment key practices
Define goals	Develop measurable outcome-based goals	Agency strategic plans should include general and outcome-based goals and objectives for major functions and operations of the agency. Performance plans should describe performance goals that are concrete, objective, and measurable.
	Assess the program environment	Agency strategic plans should include an assessment of external factors that could affect its achievement of goals and objectives.
	Identify strategies and resources	Agency strategic plans and performance plans should include a description of how goals will be achieved including operational processes, skills and technology, and the human capital, information, and other resources that will be required. Agencies are to describe actions that necessitate the involvement of other agencies.
	Involve stakeholders	At least once every 2 years, agencies should consult Congress to solicit majority and minority views from the appropriate authorizing, appropriations, and oversight committees. Agencies should also consult with stakeholders when developing or changing strategic plans.
Collect performance data	Develop performance measures	Agencies should develop performance measures used to assess the output or outcome of activities. Agencies should use these measures to determine the progress toward performance goals.
	Track information that is timely, accurate, and useful	Agencies should provide a description of processes that ensure, validate, and verify measured values. The legislative history of GPRA notes that the effectiveness of performance assessments depends on the reliability and utility of performance information. ^a

²⁰GAO, *Coast Guard: Actions Needed to Enhance Performance Information Transparency and Monitoring*, GAO-18-13 (Washington, D.C.: Oct. 27, 2017); GAO-16-393; GAO-05-927; and GAO/GGD-96-118.

Step for performance assessment	Performance assessment key practice	Description of related legal requirements that can serve as performance assessment key practices
Use performance data	Regularly communicate progress to stakeholders	Agencies should provide updates on their performance no later than 150 days after the end of the fiscal year. This is done by comparing actual performance against performance goals that were established in an agency's performance plans. Agencies are to provide frequent updates of actual performance to the Congress or program partners.
	Use data to assess progress toward goals and identify any gaps	Program officials should meet quarterly to review progress toward agency priority goals, overall trend data, and the likelihood of achieving the goal. Reviews should involve the head of the agency, the Chief Operating Officer, the Performance Improvement Officer, designated leaders for each priority goal, and relevant personnel. Reviews should assess whether activities, organizations, regulations, and policies are contributing to achieving goals.
	Identify opportunities to improve program management and results	Agencies should assess their performance against the performance plan and identify any unmet performance goals. As a part of this assessment process, agencies should explain why goals were not met and the plans and schedules for achieving unmet goals. Additionally, the assessment should include an analysis of whether the goals are impractical or infeasible, why, and provide recommended actions. Quarterly reviews should highlight and strategize areas that are at risk of not meeting goals.

Source: GAO analysis of federal legislation on program performance and related GAO reports. | GAO-23-105945

^aS. Rep. No. 103-58, at 30 (1993).

NIST Took Actions through the NICE Program to Strengthen the Cybersecurity Workforce; Selected Participants Noted Successes and Challenges

NIST has taken several actions through the NICE program to promote and coordinate a community to strengthen cybersecurity education, training, and workforce development. NIST continues to develop and seek formal community feedback to update the framework that the program developed, a reference tool used by both the public and private sectors to describe and share information about cybersecurity work. The agency also supports the program's two coordinating councils, three working groups, and four communities of interest to build and sustain a skilled cybersecurity workforce. Additionally, the program hosts numerous events throughout the year to drive coordination on cybersecurity issues across the industry, academia, and government sectors.

Focus groups of NICE community volunteers from across the industry, academia, and government sectors highlighted many program successes and challenges.

NIST Continues to Develop and Maintain the NICE Framework to Further Cybersecurity Workforce Development

The NICE program and representatives from numerous departments and agencies have worked to develop the *Workforce Framework for Cybersecurity* to further cybersecurity education, training, and workforce development.²¹ The NICE program office manages the framework and NIST officials stated that the office discusses updates at weekly staff meetings. According to NIST officials, the NICE Framework Manager schedules quarterly meetings with stakeholders to discuss the framework in more detail.

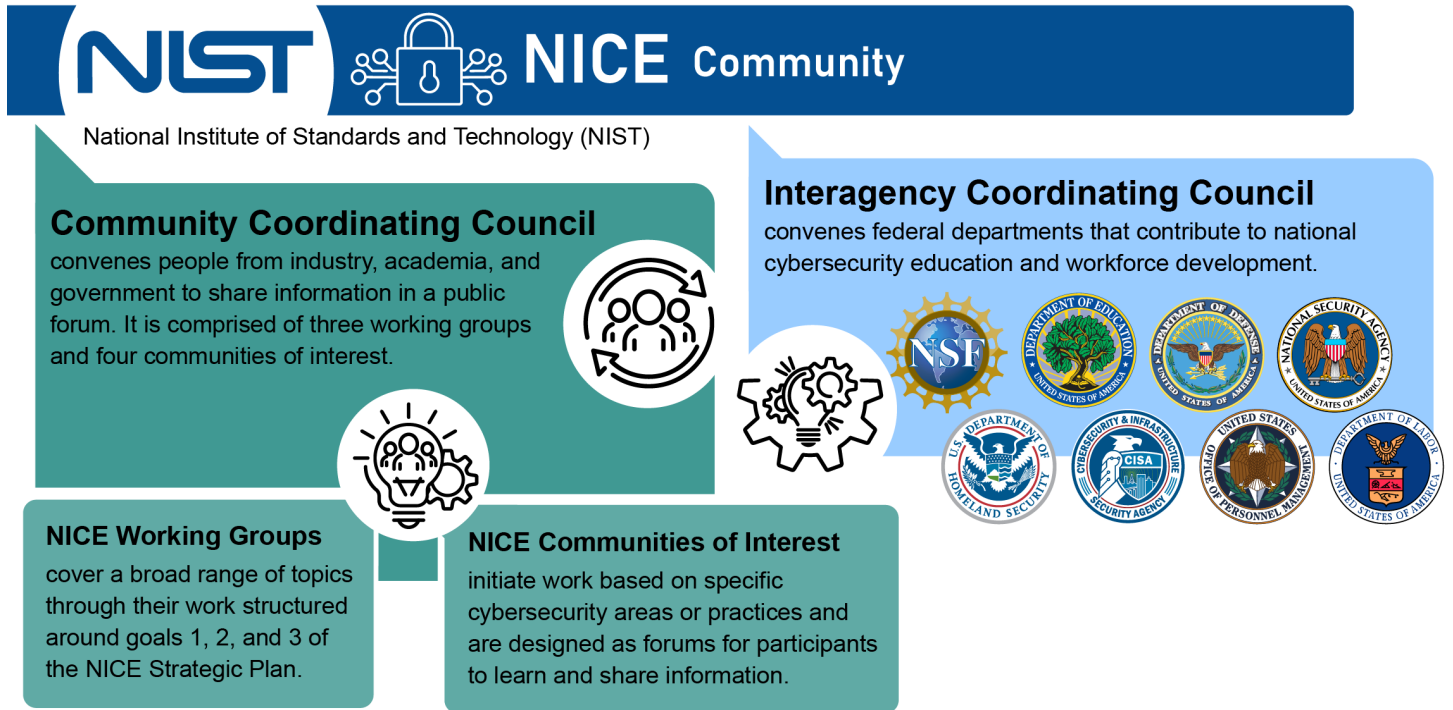
The program engages with the public and private sectors and factors in their feedback to ensure that the framework is a useful resource for their cybersecurity needs. NIST officials within the NICE program office stated that there is a formal feedback process for the framework in the form of formal requests for comments, which the office used in the 2020 framework revision. NIST officials added that the primary way the program receives feedback about the framework is through outreach, emails, or meetings scheduled with stakeholders on request to discuss how they are applying or using the framework. Additionally, the NICE Framework Users Group, a community of interest, serves as a forum to focus on sharing information and learning how to apply and use the framework.

NIST's Coordination of Councils, Groups, and Communities Advances the NICE Program Mission

NIST coordinates with the community through various means to further cybersecurity education, training, and workforce development. These coordination efforts include establishing and supporting two coordinating councils, three working groups, and four communities of interest. The two coordinating councils NIST developed are the Interagency Coordinating Council and the Community Coordinating Council. Figure 2 describes the purpose of these two coordinating councils and NICE's working groups and communities of interest.

²¹National Institute of Standards and Technology, *Workforce Framework for Cybersecurity (NICE Framework)*.

Figure 2: National Initiative for Cybersecurity Education (NICE) Interagency Coordinating Council, Community Coordinating Council, Working Groups, and Communities of Interest as of May 2023



Sources: GAO analysis of NIST information; federal agencies (logos); vektor67/stock.adobe.com (icons). | GAO-23-105945

The NICE **Interagency Coordinating Council** focuses on convening federal departments that contribute to national cybersecurity education and workforce development.²² According to NIST officials, participating agencies include the following:

- National Science Foundation
- Department of Education

²²Participation in the Interagency Coordinating Council is open to all federal employees responsible for growing and sustaining the cybersecurity workforce, which includes employees from: the Executive Offices of the President; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; and independent agencies such as the National Science Foundation and Federal Communications Commission.

-
- Department of Defense and its National Security Agency
 - Department of Homeland Security and its Cybersecurity and Infrastructure Security Agency
 - Office of Personnel Management
 - Department of Labor

NIST officials stated that the Interagency Coordinating Council typically meets 10 times each year to share information that pertains to cybersecurity education and workforce development. According to these officials, the NICE Interagency Coordinating Council aligns with the program’s mission statement of “creating an integrated ecosystem of cybersecurity education, training, and workforce development.” They stated that the council also provides input on the program’s strategic plan.

Community Coordinating Council. This council aims to convene people from academia, industry, and the government to share information—such as concepts and strategies related to the program’s mission—in a public forum. The NICE Community Coordinating Council is comprised of three working groups and four communities of interest.

Working groups. On November 5, 2020 during the NICE Conference and Expo, NIST announced a reorganization of program components along with the 2021-2025 NICE Strategic Plan.²³ The new structure converted what had been a single working group composed of subgroups into a council. The subgroups were either folded into three new working groups or converted to “communities of interest.” According to NIST officials, the working groups officially launched in February 2021. The three working groups are the following:

- Promote Career Discovery focuses on goal 1 of the Strategic Plan to promote the discovery of cybersecurity careers and multiple pathways.
- Transform Learning Process focuses on goal 2 of the Strategic Plan to transform learning to build and sustain a diverse and skilled workforce.
- Modernize Talent Management focuses on goal 3 of the Strategic Plan to modernize the talent management process to address cybersecurity skills gaps.

²³The 2020 NICE Conference and Expo was held virtually as a result of the COVID-19 pandemic.

The NICE program office tries to ensure that there is at least one individual from the private sector, academia, and government in the position of co-chairs for working groups and communities of interest. The co-chairs serve 2-year terms, with the possibility of renewal for an additional 2 years. The roles, responsibilities, and expectations for co-chairs and members of the working groups and communities of interest are laid out in the charters of these groups and communities.

Each of the three working groups has project teams that prioritize and manage new projects. These project teams focus on specific objectives within the NICE Strategic Plan and can elect to pursue some or all of the strategies to achieve objectives as laid out in the NICE Implementation Plan. Project teams have an expected duration of 6 months and, according to NIST officials, are comprised of volunteers.

The project teams may have their own charters that focus on specific strategic objectives. For example:

- The Cybersecurity Career-Entry Guidance for Employers project team was part of the Modernize Talent Management working group. This project team focused its work on strategic objective 3.3: “Align qualifications requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework.”
- The Multiple Career Pathways for Cybersecurity project team was part of the Promote Career Discovery working group. This project team focused its work on implementing objective 1.2: “Increase understanding of multiple learning pathways and credentials that lead to careers that are identified in the NICE Framework.”

Goals 4 and 5 of the NICE Strategic Plan—which center on expanding the use of the *Workforce Framework for Cybersecurity* and driving research on effective practices for cybersecurity workforce development, respectively—are not the focus of specific working groups.²⁴

Communities of interest. The four communities of interest initiate work based on specific cybersecurity areas or practices, such as cybersecurity apprenticeships and skills competitions. A realignment of working groups

²⁴For goal 4, the program has established the NICE Framework Users Group community of interest, which includes employers, learners, and credential providers. This group aims to serve as a forum in which members share information about how to implement the framework in various settings. NIST officials stated that goal 5 is integrated into the focus of all three working groups.

was part of the announcement of the new Strategic Plan at the NICE Conference in November 2020. During this realignment, some working groups, previously known as “subgroups,” were discontinued or recast as communities of interest. The Director of NICE stated that the transition to the communities of interest was determined based on demand or leadership interest. The four communities of interest are the following:

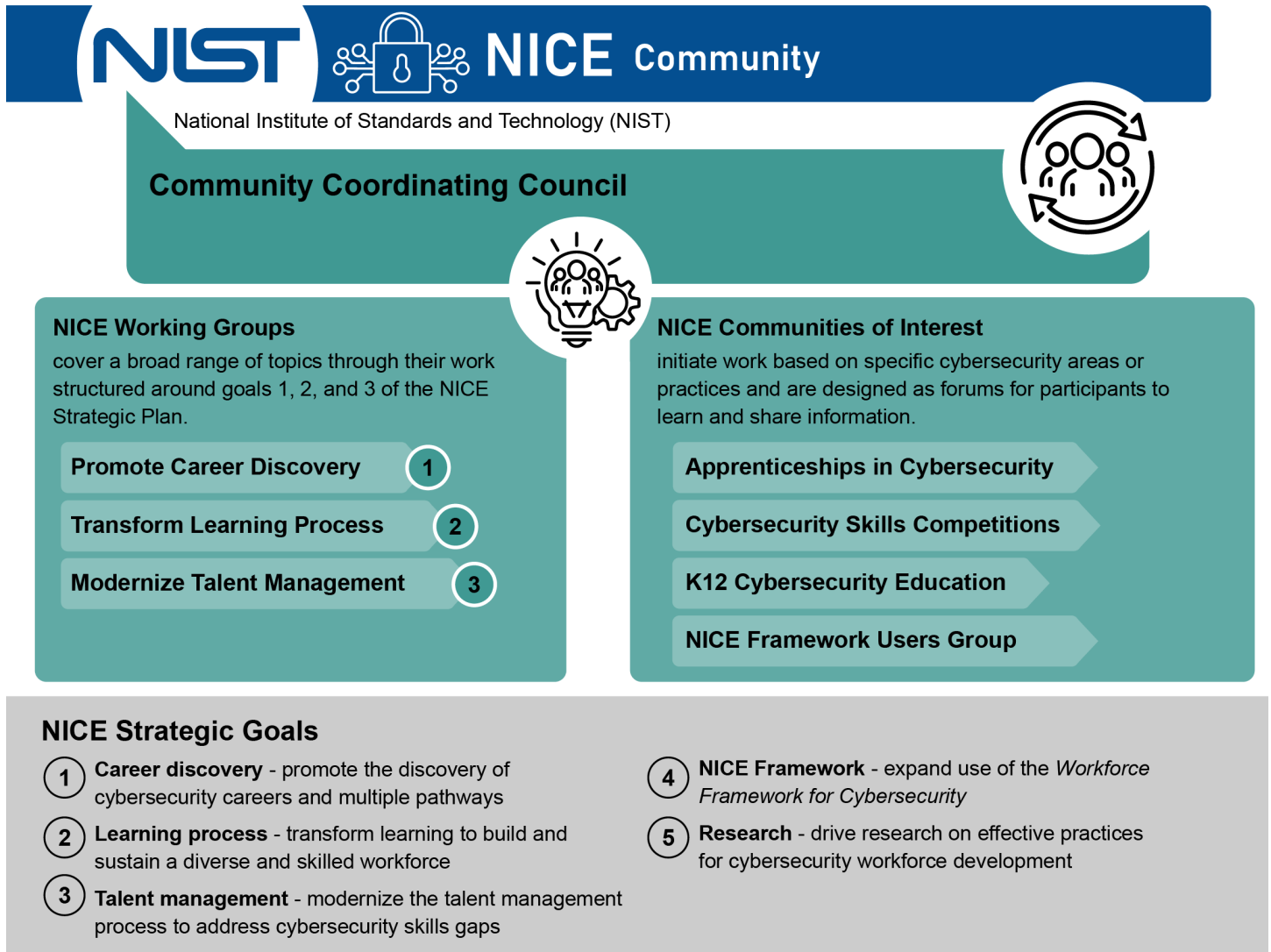
- Apprenticeships in Cybersecurity focuses on how apprenticeships work in cybersecurity related occupations.
- Cybersecurity Skills Competitions focuses on developing and promoting competitions for the public and private sectors that advance cybersecurity skills and competencies.
- K12 Cybersecurity Education focuses on growing and sustaining students pursuing cybersecurity careers.
- NICE Framework Users Group, as previously discussed, focuses on sharing information about the framework and learning how to apply and use it.

Similar to the working groups, the communities of interest center their efforts on projects. For example, the Cybersecurity Skills Competitions community of interest had the “How to Build and Run a Competition” project, which focused on creating a guide to create cybersecurity competitions. Additionally, the K12 Cybersecurity Education community of interest’s “Removing Roadblocks for Hands-on Cybersecurity Experiences in K12” project focused on creating resources that highlighted the benefits of having hands-on cybersecurity curricula and competitions in schools.²⁵

Figure 3 depicts the NICE Community Coordinating Council, which comprises three working groups and four communities of interest, and describes efforts related to the program’s five strategic goals.

²⁵NIST officials stated that the working groups focus on strategic goals and are cross-sector, include people of different backgrounds, and have a broader thematic focus. The communities of interest are silos for participants with similar interests. According to NIST officials, the communities of interest are singular in focus and reflect the needs of the communities’ constituents.

Figure 3: National Initiative for Cybersecurity Education (NICE) Working Groups and Communities of Interest with the NICE Program's Five Strategic Goals as of May 2023



Sources: GAO analysis of NIST information; NIST (logo); vektor67/stock.adobe.com (icons). | GAO-23-105945

NICE's Community Outreach Events Help Stakeholders Coordinate on Cybersecurity

The NICE program hosts numerous events throughout the year, which help further the coordination on cybersecurity issues among stakeholders from the industry, academia, and federal government sectors. According to NIST officials, the numerous events created and organized by the program align with the NICE Strategic Plan values to (1) create an

ecosystem of cybersecurity education, training, and workforce development; (2) foster communication; (3) facilitate collaboration; and (4) engage with stakeholders.

According to NIST officials, conferences and events help to connect the broader cybersecurity community by showcasing new developments and discussing successes. Events that the program hosts or otherwise coordinates are described in table 2.

Table 2: National Initiative for Cybersecurity Education (NICE) Events That the Program Hosts or Coordinates

Event	Description
NICE Conference and Expo	The expo is an annual conference for community members from education, government, industry, and nonprofits to discuss ways of developing a skilled cybersecurity workforce. The event provides an opportunity to discuss the NICE strategic plan and priorities and to showcase best practices. The inaugural conference took place in August 2010, and it has been a yearly event since 2013.
NICE K12 Cybersecurity Education Conference	This is an annual conference for K12 educators and those interested in topics surrounding cybersecurity education for the K12 youth. This conference strives to supplement attendees with knowledge about how to: increase cybersecurity awareness, integrate cybersecurity in education, and design cybersecurity academic and career pathways.
Federal Information Security Educators (FISSEA)	This organization of federal government information security—for which the NICE program assumed coordination responsibility in 2017, according to NIST officials—focuses on helping the federal agencies bolster their cybersecurity awareness and training programs. Since 2010, the organization has held an annual conference, and, in recent years, has also started to hold quarterly forums. ^a The organization, which was founded in 1987, functions as a professional forum for information sharing and to raise awareness about information systems security and training programs throughout the federal government.
Cybersecurity Career Awareness Week	This is a week intended to build awareness and promote the wide range of cybersecurity job opportunities. NIST officials stated that the NICE program was the originator of the concept for a week focused on cybersecurity careers. During the first 4 years, the event was held in November, simultaneously with National Career Development Week to highlight cybersecurity careers. The event was moved to October to coincide with Cybersecurity Awareness Month. According to NIST officials, the event was originally conceived as an initiative to directly support objective 2.3 in the 2016-2020 NICE Strategic Plan: “Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school.”
Federal Cybersecurity Workforce Summit	This summit showcases experts who share information about the federal cybersecurity workforce. NIST officials stated that in 2019, Office of Personnel Management (OPM) officials reached out to NICE program staff to request a partnership to establish the annual summit. The summit is held annually in partnership with OPM.
NICE Webinar Series	NIST officials stated that the webinars highlight topics of emerging interests. They added that the topics do not always align with a specific strategic goal or objective but instead align with NICE’s mission statement and values. Agency officials also stated that the intended audience for the NICE monthly webinars is anyone in the public who is interested in cybersecurity education, training, and workforce development. These officials stated that NICE program staff decides the topics and speakers for the webinars, and working groups can provide input as well. NICE webinars are held about 10 times a year.

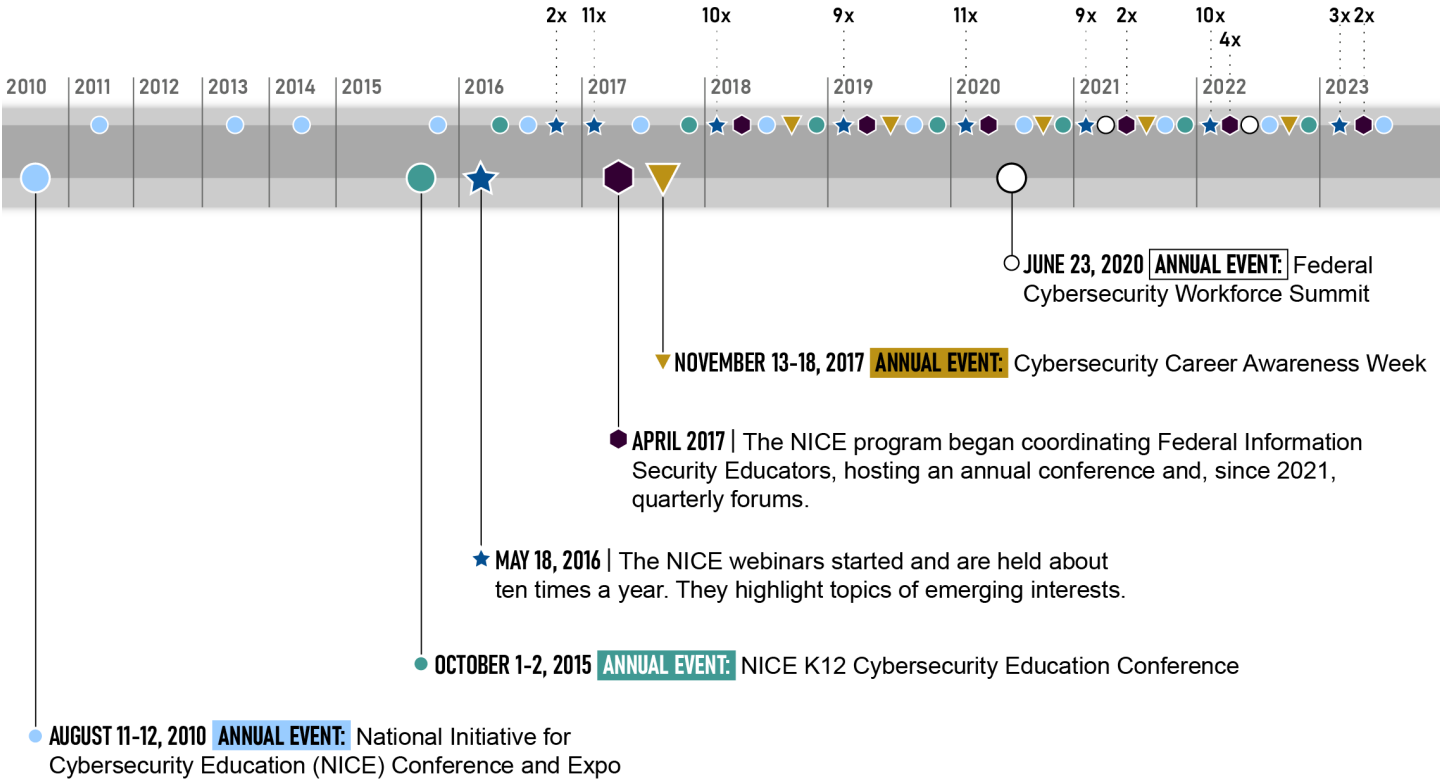
Event	Description
NICE Workshops	According to NIST officials, the workshops focus on addressing new and emerging cybersecurity issues as well as improving the <i>Workforce Framework for Cybersecurity</i> in support of the NICE program's fourth strategic goal. Agency officials stated that, typically, attendees are subject matter experts, key stakeholders, academics, or those attending due to employer interests. The webinars are scheduled with varied frequency according to NIST officials.

Source: GAO analysis of NIST documentation. | GAO-23-105945

^aFISSEA did not hold an annual conference from 2020 through 2022 due to the COVID-19 pandemic.

The first and subsequent occurrences of the NICE Conference and Expo, NICE K12 Cybersecurity Education Conference, FISSEA, Cybersecurity Career Awareness Week, Federal Cybersecurity Workforce Summit, and NICE Webinar series are depicted in figure 4.

Figure 4: First and Subsequent Occurrences of the Events the National Initiative for Cybersecurity Education (NICE) Program Hosts or Coordinates, August 2010-June 2023



x (number of occurrences [if multiple])

Source: GAO analysis of NIST information. | GAO-23-105945

In addition to organizing or hosting events, NIST officials stated that program staff also participate in and are often invited to speak at external cybersecurity events hosted by other organizations that overlap with their work. According to NIST officials, external events in which NICE staff have participated include the Community College Cyber Summit, National Centers of Academic Excellence in Cybersecurity symposia, GenCyber meetings, National Governors Association National Summit on State Cybersecurity, Women In Cybersecurity, and the RSA Conference.²⁶

Focus Group Discussions Highlighted NICE Program Successes and Challenges

Focus groups identified many successes and challenges of the NICE program.²⁷ Three of the top successes and four of the top challenges—those identified by four or more of the six focus groups—are discussed below. For a full list of success and challenge themes that the focus groups identified and examples of each, see appendix II.

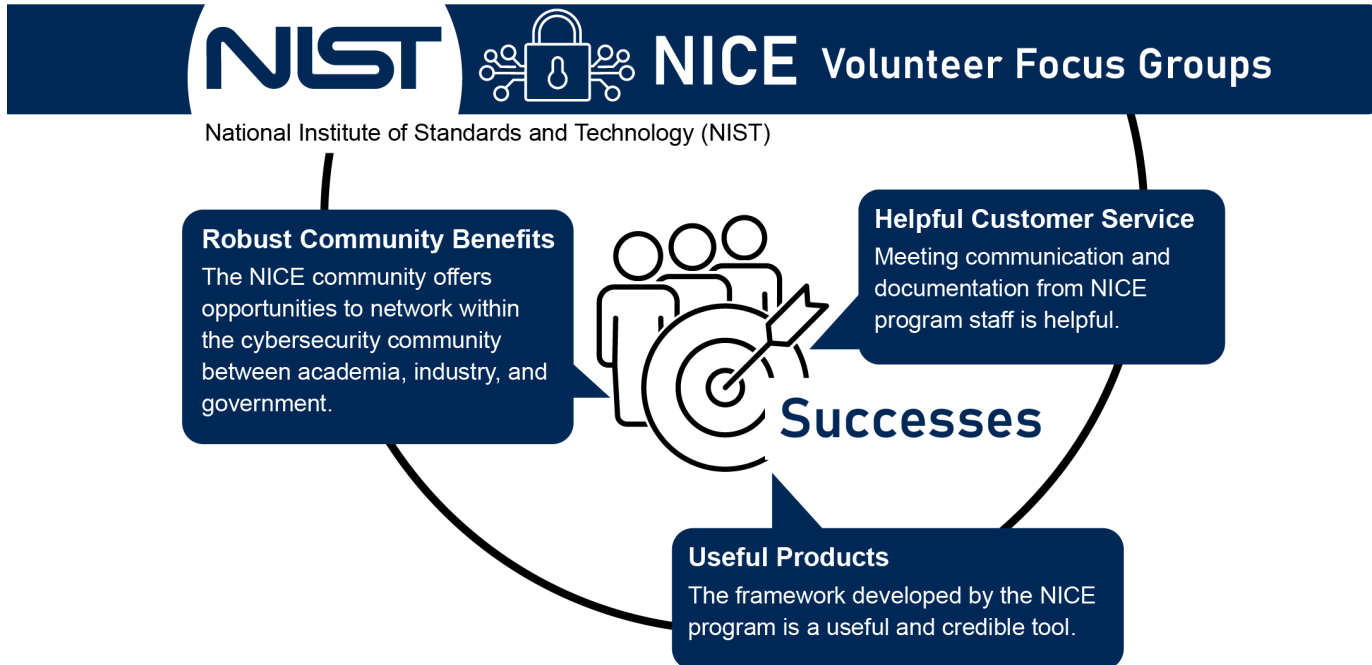
Focus Group Participants Discussed Successes of the NICE Program

According to participants across the six focus groups, helpful customer service, robust community benefits, and useful products are some of the successes of the NICE program. Figure 5 depicts examples of statements made by focus groups related to these successes.

²⁶GenCyber provides experiences, such as camps, to secondary level students and teachers to address the nation's shortfall of skilled cybersecurity professionals.

²⁷These focus groups were comprised of NICE community volunteers in industry, academia, and government, including those who held leadership roles—such as co-chairs of working groups or communities of interest—and nonleadership roles.

Figure 5: National Initiative for Cybersecurity Education (NICE) Program Successes Identified by Focus Groups of NICE Volunteers



Sources: GAO analysis of interviews with NICE volunteer focus groups; NIST (logo); vektor67/stock.adobe.com (icons). | GAO-23-105945

All Six Focus Groups Identified Helpful Customer Service as a NICE Program Success

Each of the six focus groups across three sectors mentioned NICE program successes tied to helpful customer service. Specifically, groups noted that the staff’s communication, scheduling, and documentation of meetings were helpful, as were their efforts in planning and coordinating the annual NICE Conference and Expo. For example, the industry focus group participants noted they benefited from using the expertise of the NICE program staff as working group liaisons.

Industry. The two industry focus groups cited helpful customer service as a NICE program success. Industry leadership participants stated that the NICE support staff were helpful in scheduling meetings and documenting them via meeting minutes. They also stated that the Director of NICE as well as other program staff were knowledgeable about the cybersecurity field. Some of the participants mentioned that program staff were helpful

to working groups through their involvement as liaisons. Additionally, industry nonleadership focus group participants stated that the program staff were helpful in planning and coordinating the annual NICE Conference and Expo.

Academia and government. Likewise, participants from the two academia and two government focus groups cited helpful customer service as a NICE program success. For example, the academia leadership focus group stated that the communication and meeting minutes from the program staff were helpful. Similarly, government leadership participants mentioned the program's coordination of meetings. This group discussed the benefits of meeting minutes provided by program staff in reiterating important points from meetings in a condensed form.

All Six Focus Groups Identified Successes Related to Robust Community Benefits

All six focus groups across the industry, academia, and government sectors mentioned successes of the NICE program related to robust community benefits. These successes included opportunities to network and stay current through NICE working groups, communities of interest, and events.

Industry. The two industry focus groups (leadership and nonleadership) identified community benefits as a strength of the NICE program. Specifically, industry leadership participants stated that the monthly community coordinating council meetings were a good way to stay current with cybersecurity trends and allowed people to contribute to the community. Participants across both the industry leadership and nonleadership focus groups explained that the community benefits, such as the opportunity to network, were the reasons why they joined a working group or community of interest. Industry nonleadership participants also stated that the conferences the NICE program hosted allowed them to connect with people from across the country that they would not have otherwise had the opportunity to meet.

Academia. Similarly, the two academia focus groups mentioned robust community benefits as a strength of the NICE program. Specifically, the academia leadership focus group participants mentioned that attending the community coordinating council meetings allowed them to stay current with cybersecurity news and trends. Additionally, this focus group discussed the council meetings' ability to help participants keep their

curricula up-to-date and allow students opportunities to network. Academia nonleadership participants also mentioned how the program provides spaces to exchange information. For example, academia nonleadership participants cited learning more about the context of the framework at the NICE Conference and Expo and NICE K12 Cybersecurity Education Conference. These participants also mentioned finding information about points of contact and projects on the program's resource page.

Government. The two government focus groups had similar sentiments regarding the benefit of sharing information with other cybersecurity professionals through the conferences and meetings. These groups noted the benefits of the networking opportunities provided by NICE events and the monthly meetings. Both the leadership and nonleadership focus groups discussed how the NICE program fostered a community centered on similar issues. For example, leadership focus group participants discussed how program members commonly experienced challenges in recruiting cybersecurity talent. The government nonleadership focus group also stated that working group special meetings were helpful and provided opportunities to learn. This focus group mentioned, for instance, that the program invited the Institute of Cyber Security for Society to participate in meetings on how to appropriately extend frameworks.

Most Focus Groups Highlighted Successes Tied to Useful Products

Five of six focus groups across the three sectors specified usable products as a NICE program success. Specifically, they mentioned the credibility and usefulness of the framework.

Industry. The industry leadership and nonleadership focus groups both identified useful products as a NICE program success. Specifically, industry leadership participants stated that the breakdown of the work roles and competencies within the framework was well done and was helpful in getting people from different organizations to reach a consensus about what cybersecurity jobs and career fields should look like. Nonleadership participants in industry stated that the framework was helpful because it allowed people to build tools around it using a common language. This group added that this common language allowed people to search the program's repository of resources for specific content to meet their objectives.

Academia. Likewise, the two academia focus groups cited useful products as a NICE program success. For example, academia

nonleadership participants discussed how the framework established credibility by demonstrating how their work aligned with its requirements. Additionally, academia leadership participants stated that the defined job competencies in the framework were helpful in this regard.

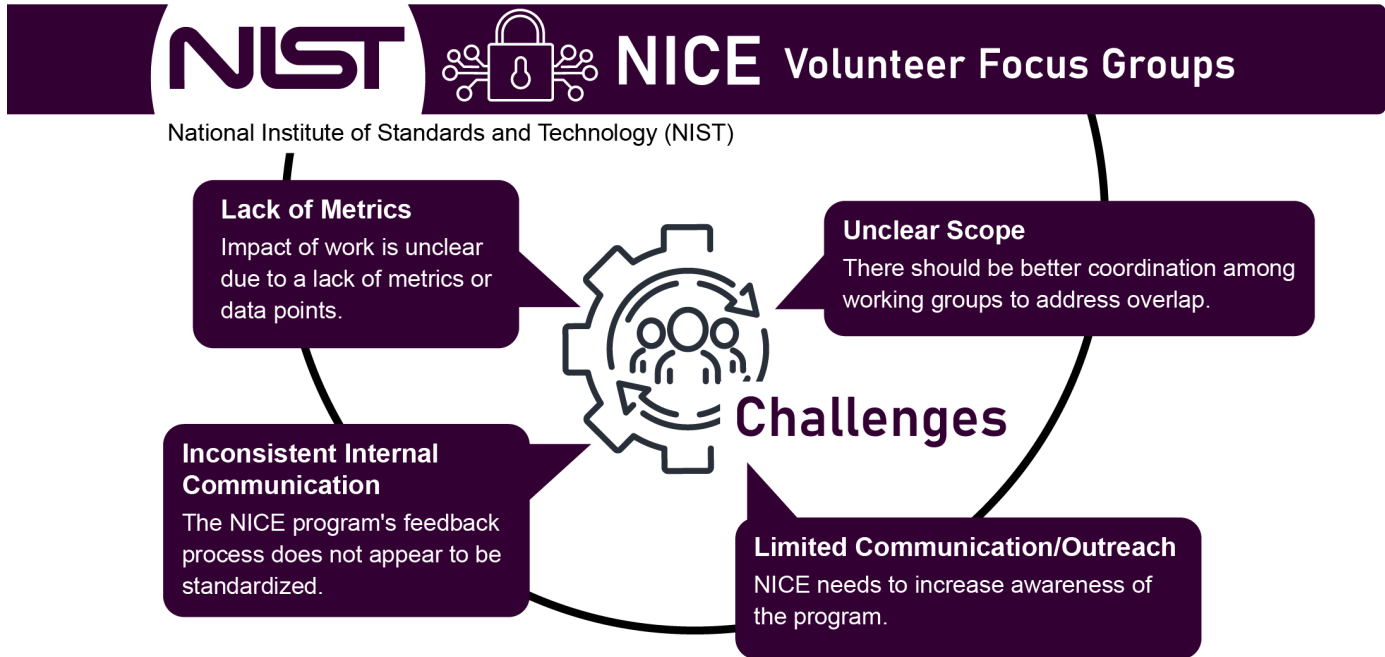
Government. Government nonleadership participants discussed benefitting from the credibility of the framework and noted that the NICE program's resources were useful as references for practitioners.

Focus Group Participants
Identified Challenges Faced by
the NICE Program

According to focus group participants in the six groups, the NICE program faced four top challenges related to (1) a lack of performance metrics, (2) limited communication and outreach, (3) unclear scope, and (4) inconsistent internal communication.²⁸ Figure 6 depicts examples of statements made by the focus groups related to these challenges.

²⁸An additional top challenge, limited information accessibility and ineffective communication strategy, cuts across aspects of both internal and external program communication. As a result, we included examples of limited information accessibility and ineffective communication strategy in the sections describing inconsistent internal communication and limited communication and outreach.

Figure 6: National Initiative for Cybersecurity Education (NICE) Program Challenges Identified by Focus Groups of NICE Volunteers



Sources: GAO analysis of interviews with NICE volunteer focus groups; NIST (logo); vektor67/stock.adobe.com (icons). | GAO-23-105945

Most Focus Groups Identified Challenges Related to a Lack of Metrics

Five of six focus groups from the industry, academia, and government sectors identified common challenges associated with the NICE program's lack of program performance metrics, such as having no clear indication of the impact of the work that NICE community volunteers completed.

Industry. The two industry focus groups (leadership and nonleadership) cited a lack of program performance metrics as a NICE program challenge. Participants across both industry focus groups stated that there were challenges in understanding the impact of the work completed by the working group project teams. Specifically, industry leadership participants stated that it was unclear what their work was used for and expressed concerns with not knowing the impact of their work.

Academia. Similarly, participants from the two academia focus groups stated that the impact of their work was unclear. These participants also discussed a lack of program performance metrics. For example, academia nonleadership focus group participants stated that there were no metrics or data points to determine how well the framework was implemented.

Government. Government nonleadership participants expressed similar concerns and stated that it would be beneficial to see performance metrics or outcomes of the work that the NICE program does.

Most Focus Groups Cited Limited Communication/Outreach as a NICE Program Challenge

Five of six focus groups from all three sectors identified several challenges related to the NICE program's limited external outreach. These challenges included the need to increase program partnerships, a lack of awareness around program marketing efforts, and the need to explain what the cybersecurity workforce is and how it works.

Industry. Participants across both the industry leadership and nonleadership groups suggested that the program should increase partnerships and awareness of the NICE program.

Academia. Academia leadership participants stated that they did not see much external outreach to entities about the Community Coordinating Council and its available resources and were not aware of any marketing that the NICE program conducted. Academia nonleadership participants suggested that it was a challenge to find which task, knowledge, and skill statements in the framework were applicable to unique student situations, such as a student majoring in English that was interested in entering the cybersecurity field.

Government. Government nonleadership participants stated that NIST officials or representatives within the NICE program should go to more events and visit programs to be more aware of recruiting efforts and provide more relevant information to young adults. Examples the nonleadership group provided included having program officials participate in more job fairs and government recruiting efforts and participating in programs such as the Scholarship for Service program. These participants stated that the program needed a way to help people understand what the cybersecurity workforce is and how it works by explaining the status of cybersecurity, how it affects people, and how it is

implemented. The government nonleadership focus group also stated that additional briefing information from the program could help bring about that cultural shift in understanding among laypeople and practitioners. Additionally, government nonleadership participants stated that the program outputs an overwhelming volume of content, making it difficult to keep up with program information. These participants stated that the program lacked a schedule for reminding people of forthcoming documents that would have allowed them to plan time to read. Moreover, the government nonleadership focus group stated that the program should have a profiling system so that people know which NICE community groups can provide the benefits that interest them.

Most Focus Groups Mentioned Unclear Scope as a NICE Program Challenge

Five of six focus groups from across the industry, academia, and government sectors highlighted multiple challenges related to the unclear scope of the NICE program and its working groups. For example, the industry leadership group mentioned the program office staff was too small to conduct the needed work to achieve the scope implied by the program's goals. Furthermore, the academia nonleadership focus group pointed out that the NICE program's coordination role may not fit with NIST's mission beyond the program's work on the framework. Additionally, the government leadership group discussed overlap across NICE working groups.

Industry. Participants in the two industry focus groups mentioned the NICE program having an unclear scope as a challenge. Specifically, industry leadership participants stated that the program was too small to conduct the amount of work needed. Moreover, the work needed exceeds the capabilities of volunteers, which causes the program to lose momentum. They stated that the program does not have enough bandwidth to do everything within the scope of its mission and goals.

Further, industry leadership participants suggested that a narrower scope would allow the program to have more impact and could help drive change quicker in the cybersecurity community. They also discussed the challenge of recruiting volunteers for project teams, noting that volunteer follow-through on projects had been a historical problem and that not many people joined the working groups or their project teams since doing so was voluntary.

Academia. Academia nonleadership participants suggested that the coordinating role of the NICE program may not fit into NIST beyond the work with the framework. Additionally, the academia nonleadership focus group stated that the program needed to figure out where it had credibility and placement to make a difference.

Government. Government leadership and nonleadership participants also identified an unclear scope as a challenge of the NICE program. Government leadership participants stated that the working groups had projects that overlapped. For example, a participant on the Promote Career Discovery working group—which works on credentialing—stated that this group’s work overlapped with other working groups’ projects. Additionally, government leadership participants noted that working groups did not have a common understanding that such overlap existed and added that expectations of the working groups should be redefined since their intent is not clear.

Moreover, government leadership participants noted that there should be better coordination among the working groups and that the program might have needed to conduct better outreach to communicate the intent of each working group. These participants discussed that the working groups were trying to do impactful work, but the work was challenging because the goals of the working groups were very large.

Most Focus Groups Discussed Challenges Tied to Inconsistent Internal Communication

While some nonleadership participants from academia said that internal communication with NICE program staff was effective and the feedback process was clear, other focus groups pointed out the lack of a clear feedback process. Four of six focus groups across the industry, academia, and government sectors discussed challenges in inconsistent internal communication with program staff and monthly coordinating council meeting participants.

Industry. The two industry focus groups noted the NICE program did not have a clearly defined process for feedback provided by working group and community of interest members. Additionally, some participants in these two groups mentioned that they were either not aware of a feedback process or did not give any feedback to program staff. Some stated that recommendations from volunteers were not always implemented.

NIST Has Taken Some Actions
to Respond to Focus Group
Perspectives

Academia. Academia leadership participants similarly discussed the lack of a clear feedback process. These participants stated that, in some cases, the ability to properly give and receive feedback was entirely dependent on the connection they had with the NICE program officials.

Government. Government leadership participants mentioned that the monthly coordinating council meetings needed to be more interactive. These participants stated that the meetings were fast paced, and co-chairs needed to have more time to debrief on the projects and work of the working groups and communities of interest. Participants in this focus group also indicated that the program's feedback process did not appear to be standardized and stated they were unsure of the program's bandwidth to receive and process feedback. Government nonleadership participants stated that it was difficult to keep up with the program due to the frequency of community meetings and that volunteers were too busy to attend all meetings that were of interest to them. Further, they stated that most program updates were not visual and were walls of text.

NIST officials within the NICE program responded that they were aware of most of the successes and challenges identified by focus groups. After reviewing a list of success and challenge themes as well as examples of each theme—shown in full in appendix II—NIST officials stated that they had taken or planned to take actions to address several challenges, including the following:

- **Lack of metrics:** During a March 2023 Community Coordinating Council leadership team meeting, NIST officials stated they shared with NICE community co-chairs metrics the NICE program office had collected for 2022, such as subscription counts for LinkedIn—a business-focused social network—and NICE Conference and Expo attendance. Meeting participants also discussed the need for working groups and communities of interest to document achievements while working toward deliverables, including through the use of success measures to gauge project team progress.
- **Limited communication and outreach:** During the March 2023 Community Coordinating Council leadership team meeting, NIST officials stated they also discussed the need for NICE program informational slides that co-chairs could share at events.
- **Unclear scope:** NIST officials stated that they planned to hold a joint meeting between the K12 Cybersecurity Education community of interest and the Transform Learning Process working group in May 2023 to address NICE community overlap challenges.

-
- **Inconsistent internal communication:** NIST officials stated they have begun to send recaps of NICE Community Coordinating Council meetings to community members, including key decisions made by council members.
 - **Undefined roles and responsibilities:**²⁹ NIST officials stated they created a webpage that used information from the NICE Community Coordinating Council charter to list roles and responsibilities of co-chairs and other members of the Community Coordinating Council. Further, NIST officials discussed roles and responsibilities of co-chairs during the March 2023 Community Coordinating Council leadership meeting.

NIST officials also made several clarifications in response to statements focus groups made regarding the following challenges:

- **Limited communication and outreach:** NIST officials stated that the NICE program had engaged in efforts to expand the program's reach in academia. These efforts included communicating with external partners such as the Center of Academic Excellence in Cybersecurity Community.³⁰ NIST officials also stated that the program had participated in job fairs such as those run by the CyberCorps® Scholarship for Service program, usually coordinating on behalf of NIST.³¹
- **Unclear scope:** NIST officials stated that the agency has taken a coordination role in capacities beyond the NICE program, including

²⁹Undefined roles and responsibilities was not one of the top four challenges above. It is discussed further in app. II.

³⁰The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program accredits two-year, four-year, and graduate-level academic institutions with the Center of Academic Excellence in Cybersecurity (CAE-C) designation based on requirements set forth by the National Security Agency, the program's sponsor. The program aims to award accreditations to institutions of higher education committed to producing cybersecurity professionals that will reduce vulnerabilities to national infrastructure. Academic institutions may pursue multiple designations—including Center of Academic Excellence in Cyber Defense, Center of Academic Excellence in Cyber Research, and Center of Academic Excellence in Cyber Operations—and must apply for redesignation every five academic years.

³¹The CyberCorps® Scholarship for Service Program provides participating institutions of higher education with scholarships to students in approved IT and cybersecurity fields of study. As a condition of receiving scholarships, students are required to enter agreements to work at qualifying federal, state, local or tribal agencies full-time jobs upon graduation for a period equal in length to their scholarship. See GAO, *Cybersecurity Workforce: Actions Needed to Improve CyberCorps Scholarship for Service Program*, [GAO-22-105187](#) (Washington, D.C.: Sept. 29, 2022).

the NIST Small Business Cybersecurity Community of Interest. NIST officials also acknowledged overlap across working groups as intentional and problematic. However, they stated that the overlap was due to crosscutting topics such as lack of standardized credentialing for cybersecurity expertise—which was an issue that the three groups needed to address.

NIST Partially Implemented Most Key Practices to Assess Program Performance

NIST performs a number of evaluative activities to assess the NICE program’s performance. However, the agency did not fully implement most of the practices derived from federal legislation and prior GAO work as key to defining goals, collecting performance data, and using performance data. Specifically, of the nine selected key performance assessment practices: NIST fully implemented one practice, partially implemented five, and did not implement three. For example, NIST officials involved stakeholders, partially developed outcome-based goals, and did not develop performance measures. As a result, NIST was unable to document with concrete, objective, measurable data any progress toward those goals or identify opportunities to improve or sustain performance.

NIST Has Partially Defined Goals for the NICE Program

NIST partially implemented key performance assessment practices for defining goals for the NICE program. Table 3 summarizes the extent to which NIST implemented each of the selected key practices for defining goals.

Table 3: NIST’s Implementation of Selected Key Performance Assessment Practices for Defining Goals for the NICE Program

Key performance assessment practices	Practice rating	Assessment of NIST’s actions
Develop measurable outcome-based goals	●	The National Initiative for Cybersecurity Education’s (NICE) 2021-2025 Strategic Plan contains high-level, long-term goals for the NICE program. In addition, National Institute of Standards and Technology (NIST) officials stated that project teams are responsible for establishing their own relevant and timely measures of success to gauge how they are advancing the program’s progress toward each strategic goal. However, NIST officials did not provide evidence to show that the NICE program had developed near-term, measurable performance goals that could mark progress toward strategic goals. NIST officials stated that inconsistency in approach and skill levels across working groups made it difficult to describe objective, concrete, and measurable performance goals. As such, these officials explained that they left the development of goals to each working group and project team. Nevertheless, NIST officials are ultimately responsible for assuring that all groups have and are meeting performance goals. Without measurable, outcome-based goals, NIST risks being unable to effectively track progress toward its strategic goals.

Key performance assessment practices	Practice rating	Assessment of NIST's actions
Assess the program environment	○	<p>NIST officials stated that they assessed the program environment through various assessment activities. For example, NIST officials stated that volunteer-led NICE Working Groups regularly assessed the program environment by conducting environmental scans, which the program office takes into consideration during strategic planning. The environmental scan that NIST provided included information on federal and nonfederal programs, projects, and initiatives. Additionally, NIST officials stated that they periodically analyzed the program's strengths, weaknesses, opportunities, and threats using an informal process involving sticky notes that they did not provide.</p> <p>However, the evidence provided did not include information on how NIST officials assessed the program-level environment for factors that may have affected the program's achievement of its strategic goals. For example, the evidence that NIST officials provided did not include how the presence of other programs affected the NICE program's achievement of its strategic goals or whether the NICE program was collaborating with identified programs. NIST officials did not include such information on factors affecting the achievement of program goals and objectives because they believed their current process for assessing the environment was enough. In not fully assessing factors and how they affect the program's achievement of its strategic goals, NIST may be less able to mitigate potential duplication of work and ensure its strategic goals are achievable.</p>
Identify strategies and resources	●	<p>NIST officials identified strategies and appropriations to achieve the NICE program strategic goals in its 2021-2025 Implementation Plan and a table of expenses that denoted how the program had spent its financial resources. NIST officials stated that they also allocated remaining resources to support grant proposals or other program priorities. Further, these officials have worked with community members to identify implementation strategies, develop or refine tactics, and determine performance measures.</p> <p>NIST officials stated they believed their current procedures were sufficient. However, while these officials did document the monetary cost of program activities, they did not identify other resource needs for the program, including human capital or other non-monetary resources for the program. Further, NIST officials did not provide a justification of the estimates and expenses related to the program's allocation of resources to the other priorities. Until the agency identifies and justifies other resource needs, including human capital, the agency may not be able to effectively plan for and allocate such resources.</p>
Involve stakeholders	●	<p>NIST officials involved stakeholders by consulting with industry, academia, and government under its community coordinating councils, working groups, and communities of interests. These groups helped develop the strategic plan and implementation plan. They have also solicited comments from the cybersecurity community to update the <i>Workforce Framework for Cybersecurity</i> and reached out to collaborate with external programs that engage in cybersecurity workforce issues.</p>

Legend:

- Full implementation = NIST evidence or documentation addressed all elements of the corresponding key practice.
- Partial implementation = NIST evidence or documentation addressed some, but not all, elements of the corresponding key practice.
- No implementation = NIST evidence or documentation did not sufficiently address any elements of the corresponding key practice.

Source: GAO analysis of NIST documentation. | GAO-23-105945

Since NIST is the lead agency coordinating the NICE program, it has the ultimate responsibility to prioritize developing measurable outcome-based goals and defining operational processes, especially if working groups

and project teams do not. Without providing such direction, NIST risks inefficient use of resources, including that of the NICE community volunteers. Until the agency documents the program’s resource needs, NIST cannot be assured it is fully considering and acting on potential barriers or facilitators for achieving its goals.

NIST Has Partially Collected Performance Data

NIST has collected some performance data on NICE program activities, but the process NIST used to assess the NICE program did not fully implement selected key practices. Table 4 summarizes the extent to which NIST implemented each of the selected key practices for collecting performance data.

Table 4: NIST’s Implementation of Selected Key Performance Assessment Practices for Collecting Performance Data for the NICE Program

Key performance assessment practices	Practice rating	Assessment of NIST’s actions
Develop performance measures	○	<p>The National Institute of Standards and Technology (NIST) did not develop program performance measures associated with NICE strategic goals and objectives. NIST officials mentioned developing personnel performance measures as part of their individual annual performance plans. While assessing staff strengths and weaknesses is instrumental to staff performance management, this level of assessment does not measure the NICE program’s overall progress toward its strategic goals. Further, the officials noted that program-level performance measures did not move beyond initial development and did not undergo review or vetting. NIST officials stated that the NICE Working Groups drafted some performance measures throughout 2021 and 2022. According to NIST officials, working groups drafted measures for project teams to further consider or refine. These officials provided examples of project team success measures that tracked project team activities and outputs. However, NIST officials did not provide documentation of a process used across the program to ensure that these measures linked to the overall NICE strategic goals for the program. Further, these officials did not provide any documentation on an established baseline for comparison with future results to see if strategic goals were met.</p> <p>NIST officials stated that they left the development of program performance measures to each project team. They also cited the inconsistent approaches and varied skill levels within project teams comprised of volunteers as challenges to developing performance measures. Further, these officials explained that due to time constraints and competing priorities, they decided to focus on the work project teams were conducting rather than developing ways to measure the performance of those teams. They stated that priorities included administrative tasks and operating a program of events, meetings, and other engagements. However, they did not specify why they were unable to make progress in establishing program performance measures several years since. Without developing and collecting program performance data with defined measures, NIST risks lacking a concrete, objective, and measurable way of assessing how the NICE program activities contribute to and meet its strategic goals.</p>

Key performance assessment practices	Practice rating	Assessment of NIST's actions
Track information that is timely/accurate/useful	●	<p>Although NIST tracked some information in the form of weekly meetings and status reports, it did not track concrete, objective, and measurable performance information due to the lack of program performance measures. NIST officials stated that they tracked performance information as part of their personnel performance process; however, as noted earlier, measuring staff performance does not measure a program's progress toward achieving its strategic goals.</p> <p>NIST officials stated that the data they already collected were sufficient, and they left the tracking of timely, accurate, and useful information to each project team. These officials also provided examples of data they have on program office activities, such as subscription counts for LinkedIn—a business-focused social network—and feedback surveys for their webinars. However, they did not explain how the data indicated progress toward achieving the NICE strategic goals, and they did not see a need to document targets or baselines for other data relating to the strategic plan goals and objectives. Further, NIST officials did not have a documented process to ensure that information they collected was accurate. Until NIST ensures a process to select and collect relevant performance data for analysis, the agency may be hindered in providing effective oversight over the NICE program as well as its volunteer-led community project teams.</p>

Legend:

- Full implementation = NIST evidence or documentation addressed all elements of the corresponding practice.
- Partial implementation = NIST evidence or documentation addressed some, but not all, elements of the corresponding practice.
- No implementation = NIST evidence or documentation did not sufficiently address any elements of the corresponding practice.

Source: GAO analysis of NIST documentation. | GAO-23-105945

A lack of established outcome-based goals inhibits the program's ability to collect relevant data to ensure effective program performance. Without performance measures and related data that are timely, accurate, and useful to track performance, NIST risks its ability to assess program activities against strategic goals and provide effective oversight for the program and project teams.

NIST Has Partially Used Performance Data

NIST used data on program activities to assess program performance, but the agency's use of data did not fully implement selected key practices for performance assessment. Specifically, NIST did not use program performance metrics to assess how program activities advanced strategic goals. Table 5 summarizes GAO's assessment of NIST's implementation of each of the selected key practices for using performance data.

Table 5: NIST’s Implementation of Selected Key Practices for Using Performance Data for the NICE Program

Key performance assessment practices	Practice rating	Assessment of NIST’s actions
Regularly communicate progress to stakeholders	●	<p>The National Initiative for Cybersecurity Education (NICE) has made publicly available on its website summaries of accomplishments and infographics. These provide an overview of program activities such as the number of developed publications, conferences, and other outreach efforts of the program. Additionally, the National Institute of Standards and Technology (NIST) provided quarterly newsletters containing updates on the program’s activities via an opt-in mailing list. Previous editions of the newsletters are available on the NICE program website. NIST officials stated that they report NICE program performance to congressional committees at least annually. These officials stated they also report progress toward goals and objectives for the program that align with Commerce’s plan semi-annually. However, these officials did not have a performance plan, a document in which program management can measure progress toward the achievement of both the annual goals linked to long-term and strategic plan goals. Additionally, the evidence they provided us did not demonstrate concrete program performance measures that would have allowed them to effectively report program performance information to stakeholders.</p> <p>NIST officials did not see the need to document a performance plan. Additionally, the evidence they provided, including personnel performance assessments, did not demonstrate program performance measures that would facilitate reporting performance information to stakeholders. Without a performance plan and relevant program performance information—such as performance measures with baselines, targets, and milestones—NIST risks its ability to efficiently and effectively communicate progress to stakeholders.</p>
Use data to assess progress toward goals, and identify any gaps	○	<p>NIST has not demonstrated the ability to assess its progress toward program performance goals due to the lack of performance measures. NIST officials stated that they tracked performance information as part of their personnel performance process. NIST also stated that they assessed program performance as a part of its Summary of Accomplishment and Impact graphics. These officials stated that they periodically met with the NICE Leadership Team to assess working group and project team progress. Additionally, they provided periodic reports on progress toward the Department of Commerce’s Strategic Plan goals. However, these examples did not demonstrate the use of concrete, objective, and measurable performance data in the assessment of the NICE program’s strategic goals.</p> <p>As previously mentioned, NIST officials were unable to demonstrate that they could use data to assess progress toward the program’s strategic goals and identify any gaps. Without using data to identify gaps, the agency risks its ability to evaluate the NICE program’s progress toward its strategic goals.</p>
Identify opportunities to improve program management and results	○	<p>NIST has not demonstrated being able to identify and implement opportunities to improve the NICE program based on measurable program performance data. The lack of program performance measures means that program management lacks the necessary information to identify underperforming areas or ineffective strategies.</p> <p>NIST officials stated that they developed and implemented solutions based on quantitative and qualitative data inputs. However, NIST officials have not provided documentation for these data inputs or any opportunities and solutions derived from them. Without program performance measures, program management lacks the necessary information to identify underperforming areas or ineffective strategies.</p>

Legend:

- Full implementation = NIST evidence or documentation addressed all elements of the corresponding practice.
- ◐ Partial implementation = NIST evidence or documentation addressed some, but not all, elements of the corresponding practice.
- No implementation = NIST evidence or documentation did not sufficiently address any elements of the corresponding practice.

Source: GAO analysis of NIST documentation. | GAO-23-105945

Because NIST officials believed the program performance assessment process they had for defining goals and collecting data was sufficient, they lacked a systemic way to use program performance data to identify improvement opportunities. Using objective, concrete, and measurable data to communicate progress to stakeholders, identify gaps, and identify opportunities, would better position NIST to provide effective oversight. Furthermore, without a systematic approach to using program performance data, NIST will be challenged to ensure that its resources are being optimally used and demonstrating the NICE program's impact on the cybersecurity workforce.

Conclusions

NIST has taken actions to coordinate a community to further cybersecurity education, training, and workforce development. Its *Workforce Framework for Cybersecurity* has enabled robust communication about the knowledge and skills needed to recruit and retain cybersecurity talent in the public and private sectors. Furthermore, the NICE program's working groups and communities of interest have worked together to build and sustain the cybersecurity workforce and promote and coordinate a cybersecurity community. These participants have also noted program challenges that NIST plans to address.

Nevertheless, NIST has not fully implemented most key practices to assess the NICE program's performance. It lacks fully developed measurable goals and performance measures, program environment assessments and strategies, reliable information to assess and communicate progress to stakeholders, and the use of data to identify opportunities for improvement. These shortfalls hinder the ability of stakeholders, program management, agency leadership, and the public to gauge the program's achievements.

Recommendations for Executive Action

We are making the following eight recommendations to NIST:

The Director of NIST should ensure that the Director of NICE develops a program performance plan with goals that are measurable. (Recommendation 1)

The Director of NIST should ensure that the Director of NICE updates the program's environmental scan documentation to include an assessment of how the outcomes and impacts of the identified programs, projects, and initiatives may affect the program's achievement of its performance plan and the strategic plan goals. (Recommendation 2)

The Director of NIST should ensure that the Director of NICE assesses and justifies the resources that the program requires to achieve its performance plan and the strategic plan goals. (Recommendation 3)

The Director of NIST should ensure that the Director of NICE establishes performance measures with a plan to collect the data needed to assess progress toward each performance goal. (Recommendation 4)

The Director of NIST should ensure that the Director of NICE regularly collects program performance information that is measurable, timely, accurate, and useful. (Recommendation 5)

The Director of NIST should ensure the Director of NICE reports measurable program performance information to stakeholders. (Recommendation 6)

The Director of NIST should ensure that the Director of NICE assesses progress toward achieving program performance goals with measurable performance information. (Recommendation 7)

The Director of NIST should ensure that the Director of NICE uses performance information to manage the program, including to identify opportunities to improve program results, as appropriate. (Recommendation 8)

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of Commerce for its review and comment. In its written comments, reproduced in appendix III, the department agreed with our recommendations and suggested wording changes, which we incorporated as appropriate. Among other things, the suggested changes involved clarifying our recommendations on the NICE program's performance assessment practices. In its comments, Commerce also noted that some aspects of recommendations 1 and 4 were redundant and suggested combining recommendations 4 and 5.

With regard to the suggestions related to recommendation 4, the department stated that the use of "establish performance measures" in recommendation 4 was redundant with recommendation 1. Therefore, we revised the wording in recommendation 1 to reflect the department's suggestions related to measurable goals in a performance plan.

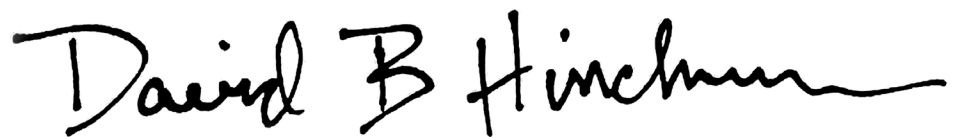
However, we did not implement the department's proposal to combine recommendations 4 and 5 because recommendation 4 included both the

establishment of performance measures and a plan for collecting them and is solely focused on the lack of program performance measures. As we previously noted, it is vital for agencies to develop performance measures to assess the output or outcomes of related activities to determine progress toward performance goals. In addition, it is important for agencies to document the processes by which they will collect the data associated with performance measures.

Further, recommendation 5 addresses the need for timely and accurate program performance information, which extends beyond any specific performance measures developed by the program. Because of this, we maintain that these recommendations should be separate so that the department can clearly demonstrate that it can collect and validate performance data. Once the department has established performance measures and planned for the collection of related data, validating and verifying such data will be key to ensuring they are timely, accurate, and useful. The department also provided technical comments that we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Commerce, the Director of NIST, and other interested parties. In addition, this report will be available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions regarding this report, please contact me at (214) 777-5719 or hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our specific objectives were to determine (1) the actions NIST has taken through the NICE program to strengthen the cybersecurity workforce, and (2) the extent to which NIST established a process to assess the program's performance.

To address the first objective, we analyzed documentation of NIST's mission, structure, and strategic goals and the history of the NICE program by conducting background research on its program site and reviewing its strategic plan and implementation plan. We reviewed the charters of each working group and its project teams as part of the analysis. We collected and analyzed monthly coordinating council, working group, and community of interest meeting agendas and meeting minutes. We reviewed documentation, such as charters, related to the creation and continuation of coordinating councils, working groups, and communities of interest.

In addition, we conducted semi-structured interviews with NICE program officials and third-party participants in the NICE program to obtain their perspectives on how the program is managed. We conducted a series of interviews and follow-ups by providing a list of questions to the Department of Commerce liaison, who then worked with the NICE program office to invite the appropriate officials to participate in interviews.

To get third-party perspectives on actions NIST has taken to further the cybersecurity workforce, we conducted focus groups with participants from NICE's Community Coordinating Council, working groups, and communities of interest. We selected a focus group methodology as a way to get in-depth answers from these NICE community participants about a variety of relevant topics, while also benefiting from the interactions among participants. As is typical with focus groups, the unit of analysis was at the group level because our intent was to identify any similarities or differences in themes that emerged from the group discussions rather than to capture individual statements or consensus among the participants.

To develop our sample frame for these groups, we first developed a list of active participants in NICE's Community Coordinating Council, working groups, and communities of interest between December 2020 and August 2022 based on the meeting minutes generated for their monthly

meetings.¹ We recorded names, contact information, working group or community of interest membership, leadership role (i.e., those who held or had held NICE working group and community of interest co-chair positions), organization, and job position. Based on their contact information and organization, we then sorted the individuals into one of three working sectors (i.e., industry, academia, and government) and, within each sector, one of two subcategories: leadership and nonleadership (those who had not held leadership positions in the NICE community). For any individuals with incomplete information, we conducted research on the internet to fill out missing fields to the extent possible. After removing duplicate names as well as ones without available email addresses, NICE officials provided and verified the contact information for members identified.

We used a randomization formula within each of the six groups to determine the order in which we reached out to volunteers to participate in focus group interviews. We then conducted a total of six focus group sessions with leadership and nonleadership volunteers from the industry, academia, and government sectors. Where possible, the focus groups consisted of three or more NICE community volunteer members, resulting in the number of participants in each focus group ranging from two to four volunteers. We worked with our methodologists to ensure the questions we developed for the focus group sessions were unbiased and phrased in a way that best elicited discussion. Topics discussed during the focus groups included the participants' history volunteering with the NICE program, NICE program staff support to volunteers, the effective actions or successes toward achieving the NICE mission, challenges observed, and areas of improvement.

To determine the themes of successes and challenges from the focus groups, we performed a content analysis using records of interviews from each session. We gathered statements relating to NICE program successes and challenges from each of the six records of interview and coded each of these statements into a shorter descriptive theme. We then sorted the short descriptive themes into more general, overarching success and challenge themes. An analyst matched each record of interview statement with a short descriptor and overarching theme. A second analyst then reviewed the assigned descriptors and themes and recorded agreement or a comment to document disagreement and

¹A sample frame is a target population from which a sample is created.

suggest a more appropriate theme. The two analysts then worked to address the comments and assign a final success or challenge theme.

For each main success and challenge theme, we recorded whether each of the six focus groups identified the theme during the focus group interview. We then calculated the number of focus groups that identified each success and challenge theme. We defined top success and challenge themes as those identified by four or more of the six focus groups. We expanded upon focus group comments related to the top success and challenge themes in the first objective. Though random selection was used to mitigate selection bias, the information gathered from the interviews and focus groups is not generalizable and is meant to provide illustrative examples.

To address the second objective, we reviewed the Government Performance and Results Act of 1993 (GPRA) and its modernization act as well as past GAO reports to analyze key practices of a program performance assessment process.² We compared performance assessment processes as described in these sources, identified common themes, and compiled shared steps among results-oriented systems that lined up with the requirements for GPRA. In consultation with methodologists and subject-matter experts, we found that a performance assessment model can be expressed in three steps:

1. **Define goals.** Identify an overall goal and the activities that would help achieve it. The strategic plan is the basic underpinning for a system of goal setting and performance management.
2. **Collect data.** Develop measures to record the progress of the activities to assess the extent to which a goal was achieved.
3. **Use data.** Use the collected information to identify potential performance shortfalls and develop the solutions needed to address them.

To complete the model, we used GPRA and past GAO reports to identify key practices that supported each of the three performance assessment

²The Government Performance and Results Act of 1993, Pub. L. No. 103-62, 107 Stat. 285 (1993), amended by the GPRA Modernization Act of 2010, Pub. L. No. 111-352, 124 Stat. 3866 (2011).

process steps (see table 1 on p. 13).³ We selected nine key practices to serve as criteria to measure the effectiveness of NIST's ability to measure the NICE program's performance. We rated the program's performance assessment activities as being fully implemented if NIST evidence or documentation related to performance assessment addressed all elements of the key practices. The activities were rated as being partially implemented if only some, but not all, elements of the key practices were addressed. We rated the activities as having no implementation when NIST's evidence or documentation did not address any elements of the key practices corresponding to each assessment step.

In addition to analyzing documentation that NIST program officials provided, we conducted follow-up interviews that further clarified NIST's activities regarding specific topics such as performance measures and management methodology for the NICE program.

We conducted this performance audit from March 2022 to July 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

³Selected key practices in program performance management came from the Government Performance and Results Act of 1993 (GPRA), the GPRA Modernization Act of 2010, and GAO, *Veterans Justice Outreach Program: VA Could Improve Management by Establishing Performance Measures and Fully Assessing Risks*, [GAO-16-393](#) (Washington, D.C.: Apr. 28, 2016); *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, [GAO-05-927](#) (Washington, D.C.: Sept. 9, 2005); and *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1, 1996).

Appendix II: NICE Program Successes and Challenges Identified by Focus Groups

Six focus groups identified many successes and challenges of the National Initiative for Cybersecurity Education (NICE) program. These focus groups were composed of individuals from the industry, academic, and government sectors who volunteer with the NICE program's community coordinating council, working groups, and communities of interest. Within each of these three sectors, we further categorized participants into subgroups of leadership (if they held or had previously held a leadership role, such as a working group or community of interest co-chair) and nonleadership (if they had not held such a role).

Table 6 shows the four success themes that the six focus groups identified for the NICE program in descending order by the number of focus groups that identified the success. In addition, the table shows examples of each success theme mentioned by the focus groups, and the focus groups that identified and did not identify each success theme.

Table 6: National Initiative for Cybersecurity Education (NICE) Program Successes Identified by Focus Groups

Success theme	Identified by						Success examples ^a
	Industry L	Industry NL	Academia L	Academia NL	Government L	Government NL	
Helpful customer service	●	●	●	●	●	●	<ul style="list-style-type: none"> The program staff was helpful and took care of scheduling meetings and providing meeting minutes. Program staff was receptive of feedback. Program liaisons were helpful.
Robust community benefits	●	●	●	●	●	●	<ul style="list-style-type: none"> Fostered community centering around similar issues. Conferences and initiatives provided a way to connect with colleagues and share information. The program workshops and webinars were helpful.
Useful products	●	●	●	●	○	●	<ul style="list-style-type: none"> The framework developed by the program is a helpful tool. The framework established credibility to align work. The program provided useful resources and information.

Appendix II: NICE Program Successes and Challenges Identified by Focus Groups

Success theme	Identified by						Success examples ^a
	Industry L	Industry NL	Academia L	Academia NL	Government L	Government NL	
General program successes	●	○	○	○	●	●	<ul style="list-style-type: none"> The program effectively promoted itself. The program is making progress. The program effectively coordinated its work.

Legend:

- = NICE volunteer focus group identified the success theme.
- = NICE volunteer focus group did not identify the success theme.
- L = Leadership
- NL = Nonleadership

Source: GAO analysis. | GAO-23-105945

^aContent in this column represents examples of each success theme mentioned by the focus groups that identified the theme.

Table 7 shows the 13 challenge themes that the six focus groups identified for the NICE program in descending order by the number of focus groups that identified the challenge. In addition, the table shows examples of each challenge theme mentioned by the focus groups, and the focus groups that identified and did not identify each challenge theme.

Table 7: National Initiative for Cybersecurity Education (NICE) Program Challenges Identified by Focus Groups

Challenge theme	Identified by						Challenge examples ^a
	Industry L	Industry NL	Academia L	Academia NL	Government L	Government NL	
Lack of metrics	●	●	●	●	○	●	<ul style="list-style-type: none"> Lack of metrics on project and working group performance. Impact of the program's work is not clear. Lack of awareness of metrics to show impact of the program.

Appendix II: NICE Program Successes and Challenges Identified by Focus Groups

Challenge theme	Identified by						Challenge examples ^a
	Industry L	Industry NL	Academia L	Academia NL	Government L	Government NL	
Limited communication and outreach	●	●	●	○	●	●	<ul style="list-style-type: none"> NIST officials needed to increase awareness of program. Broader outreach issues; more briefing information can help understanding of the program. Engagement of students and incoming workforce; program activities should become more aligned with recruiting and providing information for young adults.
Unclear scoping	●	●	○	●	●	●	<ul style="list-style-type: none"> Unclear scope for working groups and communities of interest. Overscoping/scope was too large for program size/program needed to assess its scope. Coordination role of the program may not have fit in NIST beyond its work on the framework.
Inconsistent internal communication	●	●	●	○	●	○	<ul style="list-style-type: none"> Unclear or nonexistent feedback process. No clear feedback loop; depended entirely on connections with program officials.
Limited information accessibility and ineffective communication strategy	●	○	○	●	●	●	<ul style="list-style-type: none"> Difficult to keep up with the program; monthly meetings were not enough to catch up on working group accomplishments. Lack of program schedules; the program should have had reminders ahead of time for forthcoming products. Ineffective communication tools; most program updates were not visual and were walls of text.

Appendix II: NICE Program Successes and Challenges Identified by Focus Groups

Challenge theme	Identified by						Challenge examples ^a
	Industry L	Industry NL	Academia L	Academia NL	Government L	Government NL	
Resource limitation	●	○	○	○	●	●	<ul style="list-style-type: none"> • Individuals joined community groups with selfish motivations. • Some working group or community of interest participants were underqualified. • Time commitment for volunteers; volunteers were too busy to attend all meetings of interest.
Undefined roles and responsibilities	●	○	●	○	○	●	<ul style="list-style-type: none"> • Ambiguity in co-chair roles, responsibilities, and limits; no job description or onboarding process. • Working groups were duplicating efforts.
Unevenly distributed stakeholders	●	○	●	○	○	●	<ul style="list-style-type: none"> • Imbalance of academics versus practitioners; there should have been more practitioners in the program. • Lack of engagement of industry.
Environmental limitation	○	○	○	●	○	●	<ul style="list-style-type: none"> • Duplication at federal level. • The framework does not evolve at the speed of government.
General cybersecurity issues	●	●	○	○	○	○	<ul style="list-style-type: none"> • Difficulties translating technical audience communication to non-technical audience. • Need to bring awareness and clarity about cybersecurity jobs to non-technical audiences entering the cybersecurity field. • Lack of cybersecurity content for K12.

Appendix II: NICE Program Successes and Challenges Identified by Focus Groups

Challenge theme	Identified by						Challenge examples ^a
	Industry L	Industry NL	Academia L	Academia NL	Government L	Government NL	
Inflexible culture and leadership culture	●	○	○	○	○	●	<ul style="list-style-type: none"> The program initially did not want to change work roles in the framework developed by the program; it took multiple meetings to help the program understand how the framework was incomplete. Premature definitions of work could stifle innovation from new volunteers.
Program inertia	○	○	○	○	●	●	<ul style="list-style-type: none"> NICE program was slow to achieve outcomes. Program experienced workflow issues; some program initiatives happening in parallel might have been better handled in serial.
Unclear program structure	○	○	●	○	○	●	<ul style="list-style-type: none"> Unclear roles, responsibilities, and expectations for volunteers; the program office should have encouraged people to challenge its approach. Over reliance on unpaid volunteer work.

Legend:

● = NICE volunteer focus group identified the challenge theme.

○ = NICE volunteer focus group did not identify the challenge theme.

L = Leadership

NL = Nonleadership

Source: GAO analysis. | GAO-23-105945

^aContent in this column represents examples of each challenge theme mentioned by the focus groups that identified the theme.

Appendix III: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
Office of the Acting Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

July 11, 2023

David Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW Washington, DC 20548

Dear Mr. Hinchman:

Thank you for the opportunity to respond to the GAO draft report entitled GAO-23-105945, *CYBERSECURITY WORKFORCE: National Initiative Needs to Better Assess Its Performance*.

The Department agrees with the GAO's recommendations. However, in several cases the Department believes that it would helpful to reword the recommendations to add clarity and precision. For those recommendations we offer alternate wording for your consideration. The Department will prepare a formal action plan upon issuance of GAO's final report.

If you have any questions, please contact MaryAnn Mausser, Department GAO Audit Liaison, at (202) 482-8120 or mmausser@doc.gov.

Sincerely,

JEREMY PELTER
Digitally signed by JEREMY PELTER
Date: 2023.07.11 16:59:01 -0400

Jeremy Pelter

Acting Chief Financial Officer and
Assistant Secretary for Administration

**Department of Commerce's Comments on
GAO Draft Report entitled Cybersecurity: National Initiative Needs to Better Assess its
Performance
(GAO-23-105945)**

The Department of Commerce has reviewed the draft report and we offer the following comments for GAO's consideration.

General Comments

In general, the Department agrees with the substance of recommendations but in a number of cases believes that it would be helpful to reword the recommendations to make them clearer and more precise.

Comments on Recommendations

The Government Accountability Office (GAO) made eight recommendations to the Department of Commerce in the report.

- **Recommendation 1:** The Director of NIST should ensure that the Director of NICE develops program performance goals that are measurable.

Commerce Response: The Department of Commerce agrees that it is important to develop measurable performance goals, but believes that this should be part of an overall performance plan.

We therefore propose rewording this recommendation as follows: The Director of NIST should ensure that the Director of NICE develops a program performance plan with goals that are measurable.

Comment: This change moves up the "development of a program performance plan" from Recommendation 6 (develop a plan with measurable goals) since it seems more appropriate here.

- **Recommendation 2:** The Director of NIST should ensure that the Director of NICE updates the program environment documentation to include an assessment of how identified factors may affect the program's achievement of its strategic goals.

Commerce Response: The Department of Commerce agrees that it is important to update the program environment documentation and suggest adding clarification for some terms and suggest language to make this recommendation consistent with the language for Recommendation 1.

We therefore propose rewording this recommendation as follows: The Director of NIST should ensure that the Director of NICE updates the program's environmental scan

**Appendix III: Comments from the Department
of Commerce**

documentation to include an assessment of how the outcomes and impacts of the identified programs, projects, and initiatives may affect the program’s achievement of its performance plan and the strategic plan goals.

Comment: The reference to “program environment documentation” is vague and not understood; we assume you mean our “environmental scan”. The term “identified factors” is also not understood; therefore, we recommend replacing with “the outcomes and impacts of the identified programs, projects, and initiatives”. We are also inserting “performance plan” to ensure continuity with Recommendation 1. We are also using both the “performance plan” (within the NICE Program Office’s control) and “strategic plan goals” (largely outside of NIST’s direct control because of the dependency on volunteers and the contributions from academia, industry, and other parts of government).

- **Recommendation 3:** The Director of NIST should ensure that the Director of NICE assesses and justifies the resources that the program requires to achieve its strategic goals.

Commerce Response: The Department of Commerce agrees that it is important to assess and justify the program resource requirements and suggest language to ensure consistency of the recommendation with the other recommendations.

We therefore propose rewording this recommendation as follows: The Director of NIST should ensure that the Director of NICE assesses and justifies the resources that the program requires to achieve its performance plan and the strategic plan goals.

Comment: This change reflects a similar comment as above, recognizing the distinction between program office performance and successful implementation of the strategic plan.

- **Recommendation 4:** The Director of NIST should ensure that the Director of NICE establishes performance measures with a plan to collect the data needed to assess progress toward each performance goal.

Commerce Response: The Department of Commerce agrees that it is important to establish performance measures with a plan for data collection and suggest language to ensure consistency of this recommendation with other recommendations.

We therefore propose rewording this recommendation as follows: The Director of NIST should ensure that the Director of NICE establishes a plan and collects program performance information that is measurable, timely, accurate, and useful.

Comment: Use of “establish performance measures” is redundant with Recommendation 1 so we propose removing it here. Additionally, we recommend combining Recommendation 4 and 5 since they are similar (i.e., develop a data plan and collect information).

- **Recommendation 5:** The Director of NIST should ensure that the Director of NICE regularly collects program performance information that is measurable, timely, accurate, and useful.

Appendix III: Comments from the Department of Commerce

Commerce Response: The Department of Commerce agrees that it is important to collect program performance information and as per our comments on previous recommendations, we suggest the language of this recommendation be consolidated into Recommendation 4.

Comment: Per previous recommendation, we suggest combining due to the similar nature.

- **Recommendation 6:** The Director of NIST should ensure that the Director of NICE develops a performance plan and regularly reports measurable program performance information to stakeholders.

Commerce Response: The Department of Commerce agrees that it is important to develop a performance plan and report on measurable program performance information. Per our previous comments, we suggest that the portion of the recommendation related to the performance plan be added to Recommendation 1.

We therefore propose rewording this recommendation as follows: The Director of NIST should ensure that the Director of NICE reports measurable program performance information to stakeholders.

Comment: The phrase “develops a performance plan” is redundant with Recommendation 1. We also recommend moving this recommendation to follow the next goal since it would sequentially follow (i.e., we can’t report performance to stakeholders until we assess progress.)

- **Recommendation 7:** The Director of NIST should ensure that the Director of NICE assesses progress toward achieving goals for the program with measurable performance information.

Commerce Response: The Department of Commerce agrees that it is important to assess program progress and suggest an edit to the recommendation language to ensure consistency with other recommendations.

We therefore propose rewording this recommendation as follows: The Director of NIST should ensure that the Director of NICE assesses progress toward achieving program performance goals with measurable performance information.

Comments: The change to “program performance goals” is more consistent with Recommendation 1.

- **Recommendation 8:** The Director of NIST should ensure that the Director of NICE uses performance information to manage the program, including to identify opportunities to improve program results, as appropriate.

Commerce Response: The Department of Commerce agrees with this recommendation.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman, (214) 777-5719 or HinchmanD@gao.gov

Staff Acknowledgments

In addition to the contact listed above, the following staff made significant contributions to this report: Tammi Kalugdan (Assistant Director), David Hong (Analyst in Charge), Amanda Andrade, Lauri Barnes, Tracey Bass, Chris Businsky, Lilia Chaidez, Garret Chan, Andrew Erickson, Irene Li, Benjamin Licht, Ashley Mattson, Rebecca Sero, Priscilla Smith, and Andrew Stavisky.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

