



CISA Cybersecurity Performance Goals (CPG) Assessment

Missouri Department of Public
Safety/Office of Homeland Security

Download the CSET

- To complete the CISA CPG Assessment, you will need to download and install the Cyber Security Evaluation Tool (CSET) at the link below:
 - <https://www.cisa.gov/downloading-and-installing-cset>
- If you already have the CSET downloaded, you can skip this step



The screenshot shows the CISA website header with the logo on the left, the text "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE" in the center, and a search bar on the right. Below the header is a navigation menu with "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". The breadcrumb trail reads "Home / Topics / Industrial Control Systems / Downloading and Installing CSET". Social media share icons for Facebook, X, LinkedIn, and Email are visible. The main heading is "Downloading and Installing CSET". A decorative blue line with diamond ends is below the heading. The text describes CSET as a desktop software tool for evaluating industrial control system (ICS) and information technology (IT) network security practices. A blue button at the bottom left says "DOWNLOAD THE LATEST VERSION OF CSET." with an external link icon.



Download the CSET

- Under “Assets” select and download the CSET

CSET v12.4.0.4 Latest

What's new:





- Bug fixes for the CRR Report. Options for Consideration was not being populated correctly in some cases.

Algorithm: SHA256

Hash: EFB4B3E361D70D09B4284275262E92252F3F4F299D70ED8944544722D95F3C21

Path: CSETStandAloneV12404.exe

▼ Assets 3

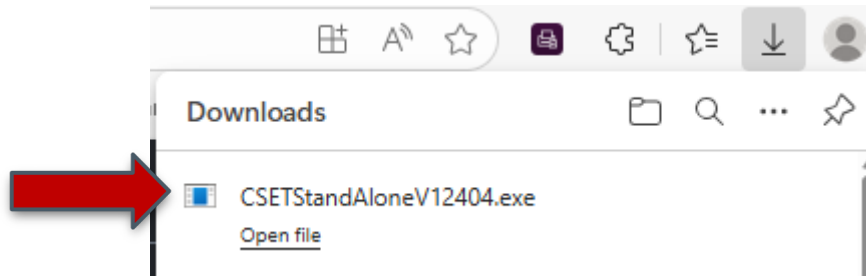
 CSETStandAloneV12404.exe	sha256:efb4b3e361d70d09b...		1.34 GB	Jul 18, 2025
 Source code (zip)				Jun 26, 2025
 Source code (tar.gz)				Jun 26, 2025

 3  3 3 people reacted



Download the CSET

- Select the tool from your downloads and download the tool to your computer



Starting an Assessment

- After the tool is downloaded, select “Start a New Assessment”



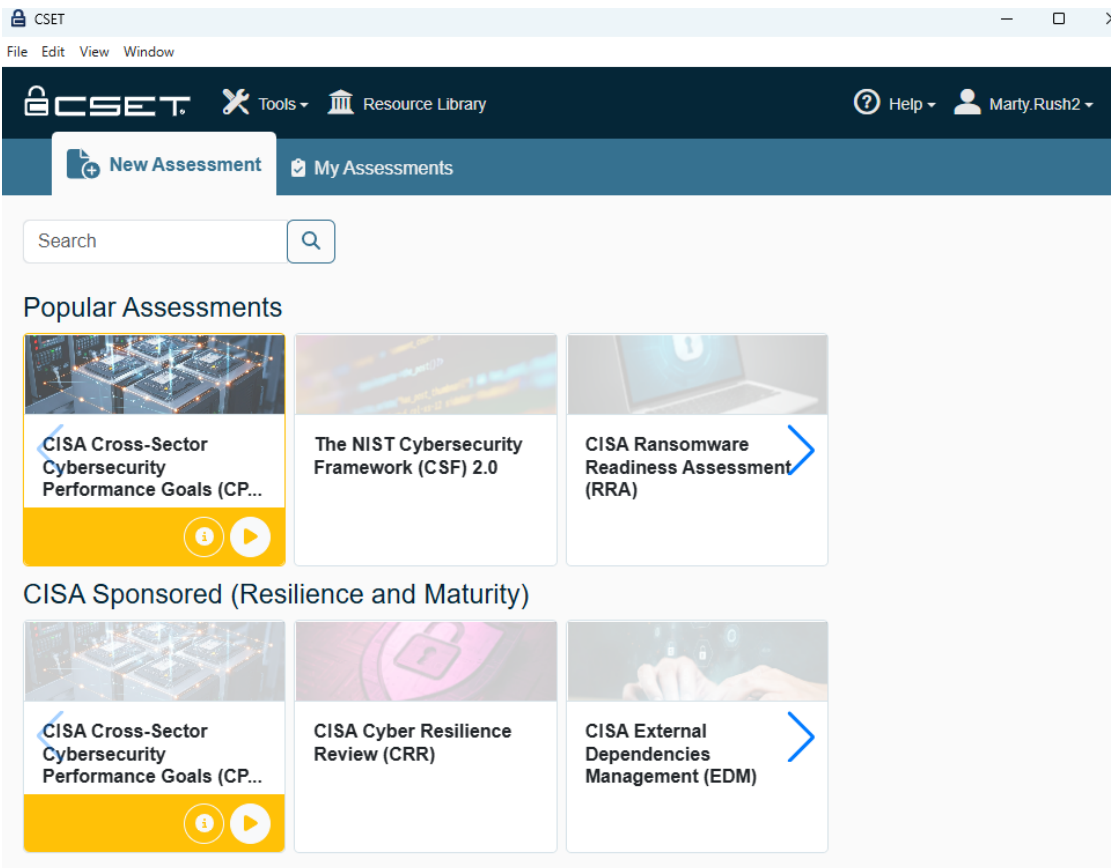
The screenshot shows the CSET web application interface. At the top, there is a navigation bar with the CSET logo, a 'Tools' dropdown menu, a 'Resource Library' icon, a 'Help' icon, and a user profile for 'Marty.Rush2'. Below the navigation bar, there are two tabs: 'New Assessment' and 'My Assessments'. The main content area is titled 'Welcome to CSET' and contains the text 'To get started, select from one of the options below:'. There are two buttons: a blue button labeled 'Start a New Assessment' and a grey button labeled 'Import an Existing Assessment'. A red arrow points to the 'Start a New Assessment' button. Below the buttons, there is a paragraph of text describing the tool.

The Cyber Security Evaluation Tool (CSET®) is a Cybersecurity & Infrastructure Security Agency (CISA) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of CISA by cybersecurity experts. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.



Starting an Assessment

- Select the arrow that looks like a “play” button on the “CISA Cross-Sector Cybersecurity Performance Goals (CPG) Assessment to create an assessment



The screenshot shows the CSET web application interface. The browser window title is "CSET". The navigation bar includes "CSET", "Tools", "Resource Library", "Help", and "Marty.Rush2". Below the navigation bar, there are tabs for "New Assessment" and "My Assessments". A search bar is present. The main content area is divided into two sections: "Popular Assessments" and "CISA Sponsored (Resilience and Maturity)".

In the "Popular Assessments" section, there are three cards:

- CISA Cross-Sector Cybersecurity Performance Goals (CP...)**: This card has a yellow bar at the bottom with a play button icon. A red arrow points to this play button.
- The NIST Cybersecurity Framework (CSF) 2.0**
- CISA Ransomware Readiness Assessment (RRA)**

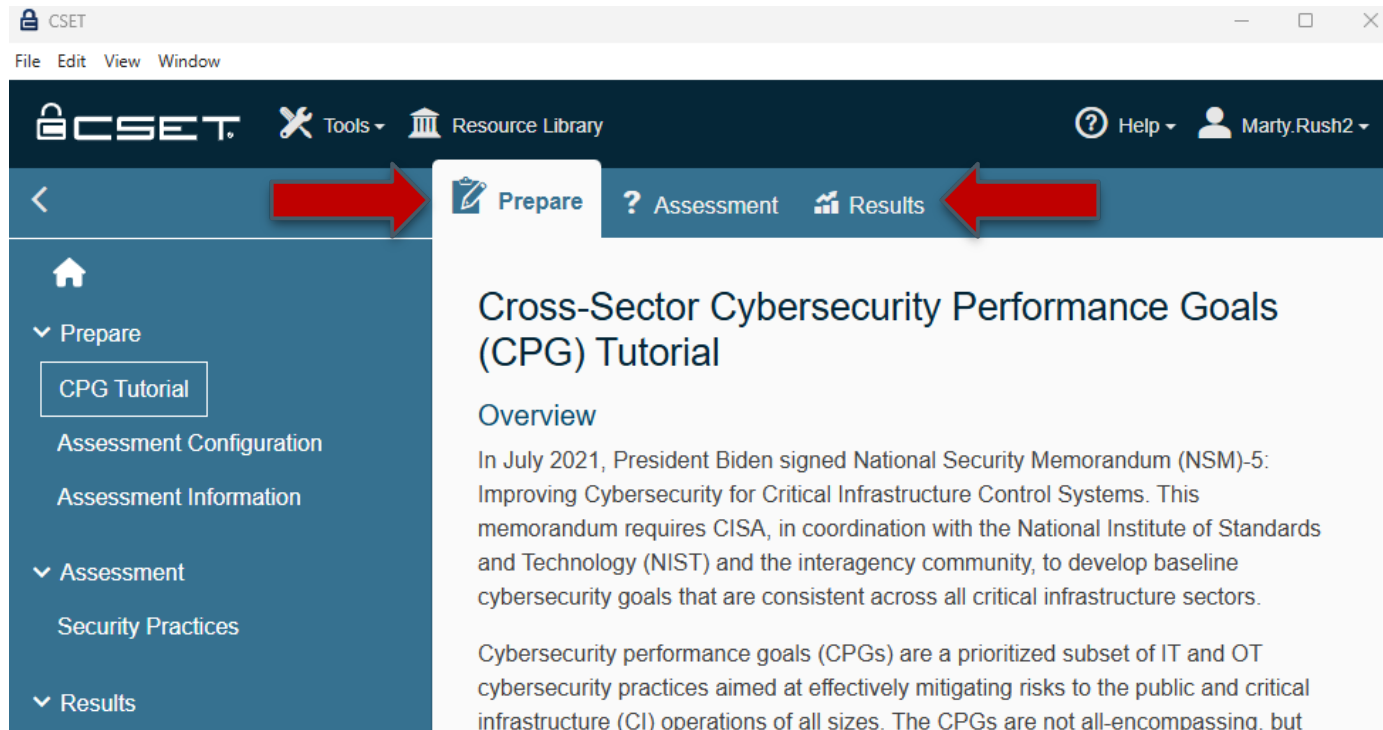
In the "CISA Sponsored (Resilience and Maturity)" section, there are three cards:

- CISA Cross-Sector Cybersecurity Performance Goals (CP...)**: This card has a yellow bar at the bottom with a play button icon.
- CISA Cyber Resilience Review (CRR)**
- CISA External Dependencies Management (EDM)**



Assessment Overview

- There will be three tabs at the top of the assessment
 - Prepare – this is a tutorial page that will provide instructions and assist you in completing the assessment
 - Assessment – this is where you will complete the assessment
 - Results – this is where you will obtain your results after the assessment is completed




The screenshot displays the CSET assessment interface. At the top, there is a navigation bar with the CSET logo, a 'Tools' dropdown, a 'Resource Library' icon, a 'Help' icon, and a user profile 'Marty.Rush2'. Below this is a secondary navigation bar with three tabs: 'Prepare', 'Assessment', and 'Results'. Red arrows point to each of these tabs. The 'Prepare' tab is currently active, showing a 'Cross-Sector Cybersecurity Performance Goals (CPG) Tutorial' with an 'Overview' section. The left sidebar contains a home icon and a list of menu items: 'Prepare' (with a sub-item 'CPG Tutorial'), 'Assessment Configuration', 'Assessment Information', 'Assessment' (with a sub-item 'Security Practices'), and 'Results'.



CPG Tutorial

- The CPG Tutorial provides an overview and background information on the CISA CPG Assessment

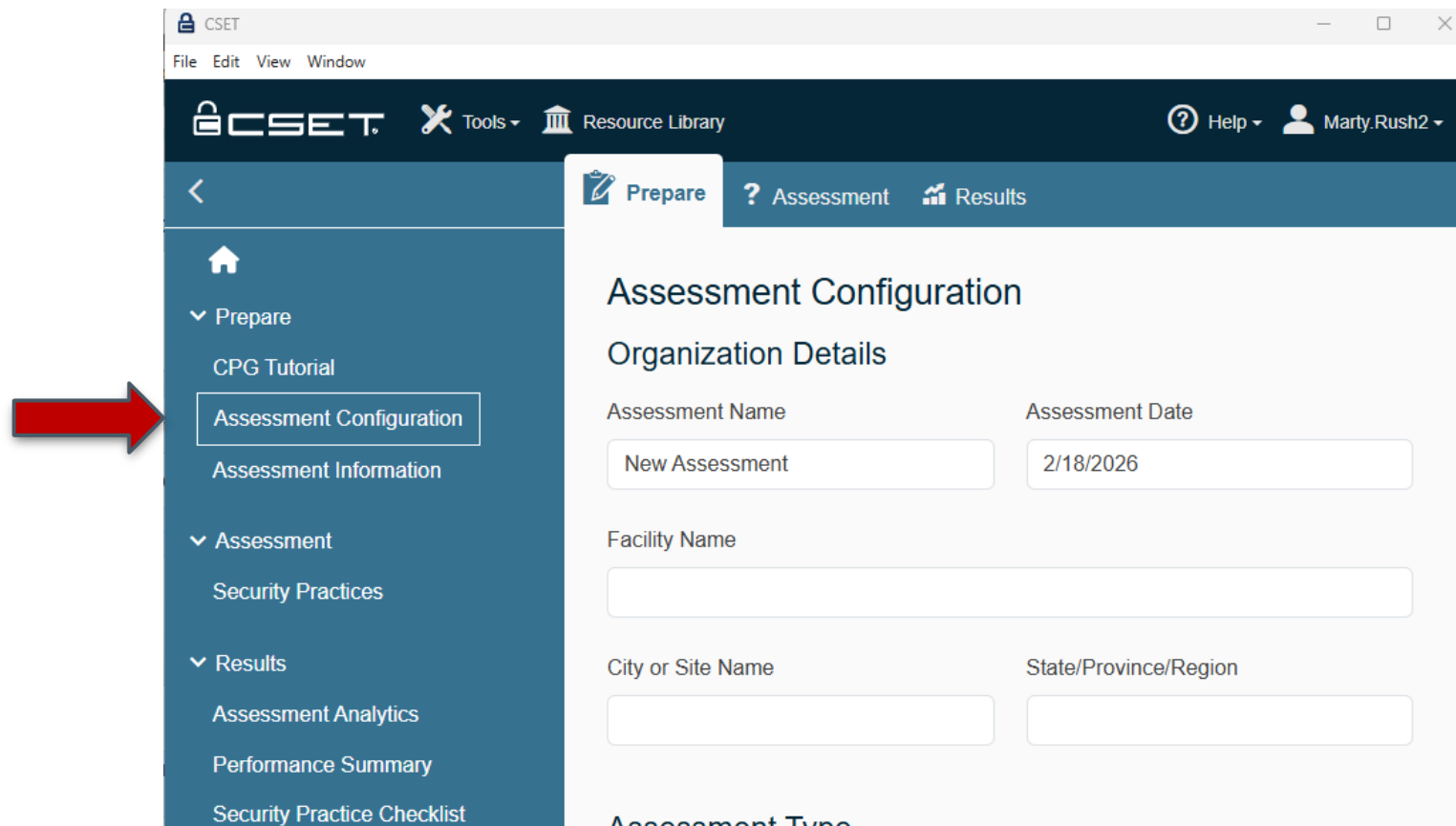


The screenshot shows the CSET application interface. The browser window title is "CSET". The top navigation bar includes "File", "Edit", "View", and "Window". The main header features the CSET logo, "Tools", "Resource Library", "Help", and a user profile "Marty.Rush2". The left sidebar is expanded to show the "Prepare" section, with "CPG Tutorial" highlighted by a red arrow. The main content area displays the "Cross-Sector Cybersecurity Performance Goals (CPG) Tutorial" page, which includes an "Overview" section. The overview text states: "In July 2021, President Biden signed National Security Memorandum (NSM)-5: Improving Cybersecurity for Critical Infrastructure Control Systems. This memorandum requires CISA, in coordination with the National Institute of Standards and Technology (NIST) and the interagency community, to develop baseline cybersecurity goals that are consistent across all critical infrastructure sectors." Below this, it defines CPGs as a prioritized subset of IT and OT cybersecurity practices aimed at mitigating risks to public and critical infrastructure (CI) operations.



Assessment Configuration

- You can configure the assessment with a name, date, facility, etc. in the “Prepare” section under Assessment Configuration

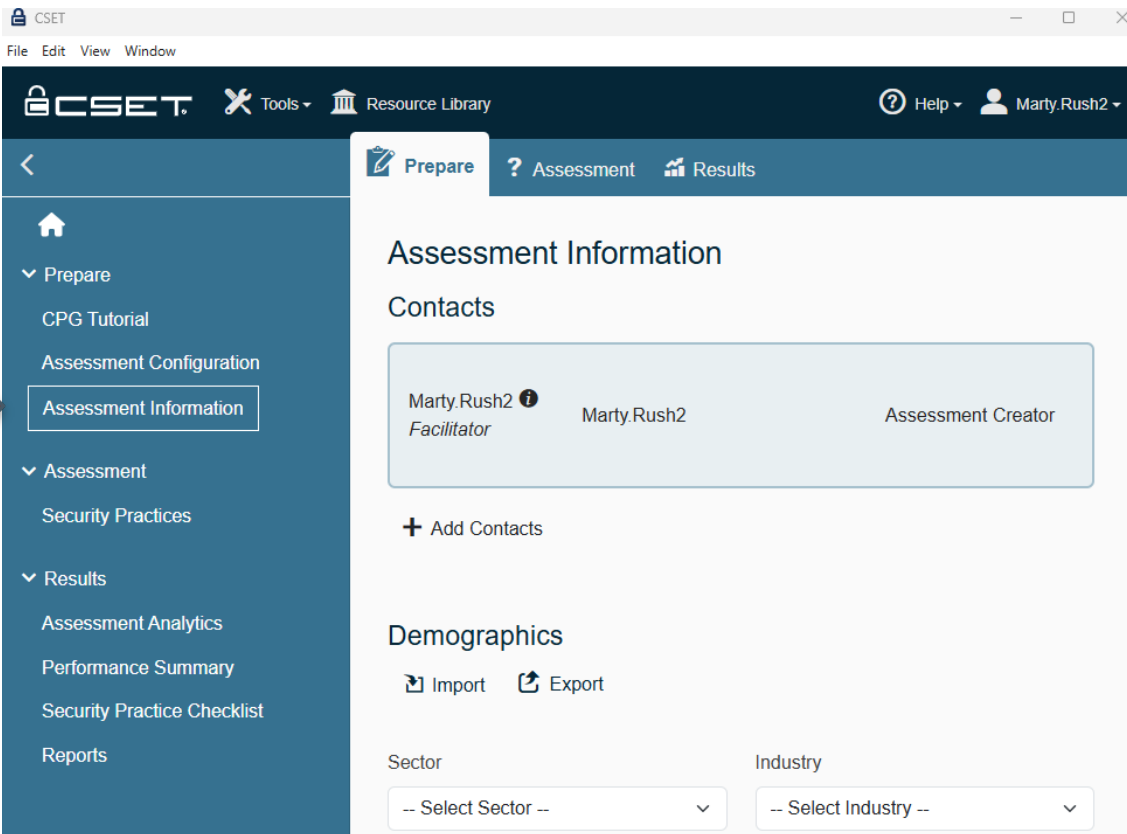


The screenshot displays the CSET web application interface. The browser window title is 'CSET'. The top navigation bar includes 'File', 'Edit', 'View', and 'Window' menus, along with 'CSET.' logo, 'Tools', 'Resource Library', 'Help', and a user profile 'Marty.Rush2'. The main content area is titled 'Assessment Configuration' and is divided into three tabs: 'Prepare', 'Assessment', and 'Results'. The 'Prepare' tab is active. The left sidebar contains a navigation menu with the following items: 'Prepare' (expanded), 'CPG Tutorial', 'Assessment Configuration' (highlighted with a red arrow), 'Assessment Information', 'Assessment' (expanded), 'Security Practices', 'Results' (expanded), 'Assessment Analytics', 'Performance Summary', and 'Security Practice Checklist'. The main content area under the 'Prepare' tab shows the 'Assessment Configuration' form with the following fields: 'Assessment Name' (value: New Assessment), 'Assessment Date' (value: 2/18/2026), 'Facility Name' (empty), 'City or Site Name' (empty), and 'State/Province/Region' (empty).



Assessment Information

- The Assessment Information section under “Prepare” will allow you to add contacts and demographics regarding the assessment



The screenshot displays the CSET web application interface. The browser window title is "CSET". The top navigation bar includes "File", "Edit", "View", and "Window". The main header features the CSET logo, "Tools", "Resource Library", "Help", and a user profile for "Marty.Rush2". The left sidebar contains a navigation menu with the following items: Home, Prepare (expanded), CPG Tutorial, Assessment Configuration, Assessment Information (highlighted with a red arrow), Assessment (expanded), Security Practices, Results (expanded), Assessment Analytics, Performance Summary, Security Practice Checklist, and Reports. The main content area is titled "Assessment Information" and is divided into two sections: "Contacts" and "Demographics". The "Contacts" section shows a table with one entry: Marty.Rush2 (Facilitator) with the role of Assessment Creator. Below the table is a "+ Add Contacts" button. The "Demographics" section includes "Import" and "Export" buttons, and two dropdown menus for "Sector" and "Industry", both currently set to "-- Select Sector --" and "-- Select Industry --".



Assessment Completion

- The CPG assessment consists of 38 security practices (questions) that align to one of the five NIST functions
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover
- Each security practice contains the following components
 - Function – NIST Function
 - Practice Identifier – Each question has an assigned practice identifier
 - Security Practice – The mitigation(s) that organizations should implement to achieve the corresponding outcome and reduce the impact of the associated risk
 - Outcome – The intended outcome that the associated security practice aims to achieve



Assessment Completion

- CSET Icons



- Supplemental Guidance Icon provides information on:
 - Scope – The set or subset of assets to which organizations should apply to the security practice
 - Recommended Action – Example approaches to help organizations progress toward achievement of the performance goal
- References Icon provides information on:
 - NIST CSF Reference – CSF subcategory that most closely relates to the security practice
 - TTP/Risk Addressed – Either the primary set of MITRE ATT&CK TTPs or the set of organizational risks that would be rendered less likely or impactful if the goal is implemented



Assessment Completion

- Answer Buttons



- For each question, select the applicable answer:

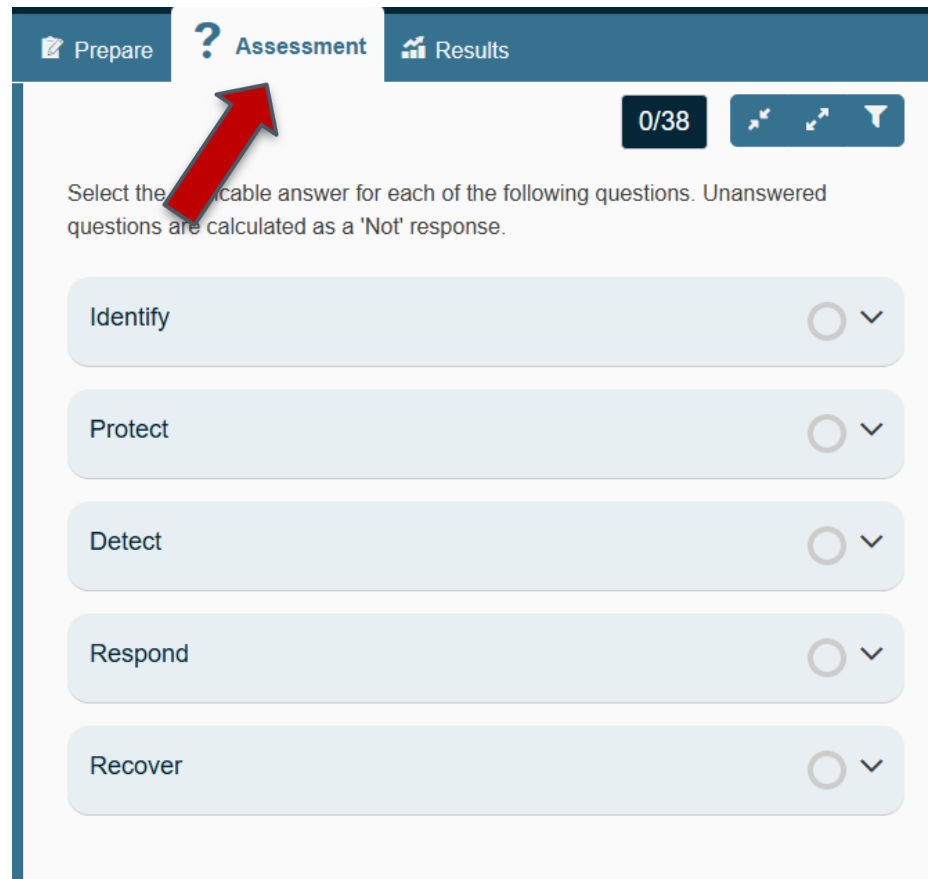
- Implemented – An organization has implemented and continues to maintain the recommended actions, or a suitable alternative, necessary to achieve the stated outcome
 - In Progress – An organization is in the process of implementing the recommended actions within a goal, or a suitable alternative, to achieve the stated outcome
 - Scoped – An organization has identified the full set of activities required to meet the stated outcome of a goal
 - Not Implemented – An organization has no immediate plans to implement the recommended actions for a goal

**Unanswered questions are calculated as a “Not” response



Assessment Completion

- To begin the assessment, select “Assessment” at the top of the page



The screenshot shows a web interface for an assessment. At the top, there is a navigation bar with three tabs: 'Prepare', 'Assessment', and 'Results'. The 'Assessment' tab is currently selected and highlighted in a darker blue. A red arrow points to the 'Assessment' tab. To the right of the tabs, there is a progress indicator showing '0/38' and three icons: a refresh icon, a share icon, and a filter icon. Below the navigation bar, there is a text prompt: 'Select the applicable answer for each of the following questions. Unanswered questions are calculated as a 'Not' response.' Below this prompt, there are five question items, each in a light blue rounded rectangle with a dropdown arrow on the right: 'Identify', 'Protect', 'Detect', 'Respond', and 'Recover'.



Assessment Completion

- Select a “NIST” Category and answer each question using the answer buttons until all questions in each category are completed

Select the applicable answer for each of the following questions. Unanswered questions are calculated as a 'Not' response.

Identify



Protect



Detect



Respond



Recover



Imp

Prog

Scoped

Not



Assessment Completion

- Below is an example of the questions when you expand a NIST Category

Identify ✓ ^

1.A **Security Practice** Imp Prog Scoped Not 🚩
Asset Inventory

Outcome
Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.

📘 💬 📄 📖 💡 🗨️

1.B **Security Practice** Imp Prog Scoped Not 🚩
Organizational Cybersecurity Leadership

Outcome
A single leader is responsible and accountable for cybersecurity within an organization.

📘 💬 📄 📖 💡 🗨️



Assessment Completion

- After all questions have been answered, there are several options to review results:
 - Assessment Analytics
 - Performance Summary – the information contained in the Performance Summary will be submitted in your Application and the Status Report in WebGrants annually, if awarded funding
 - Security Practice Checklist
 - Reports – the CPG Report will need to be printed to PDF and attached in your Application and the Status Report in WebGrants annually, if awarded funding

*You can move through the results options by selecting “Next” in the bottom right-hand corner of the screen, or from the options under the “Results” section on the left-hand of the screen

Prepare Assessment Results

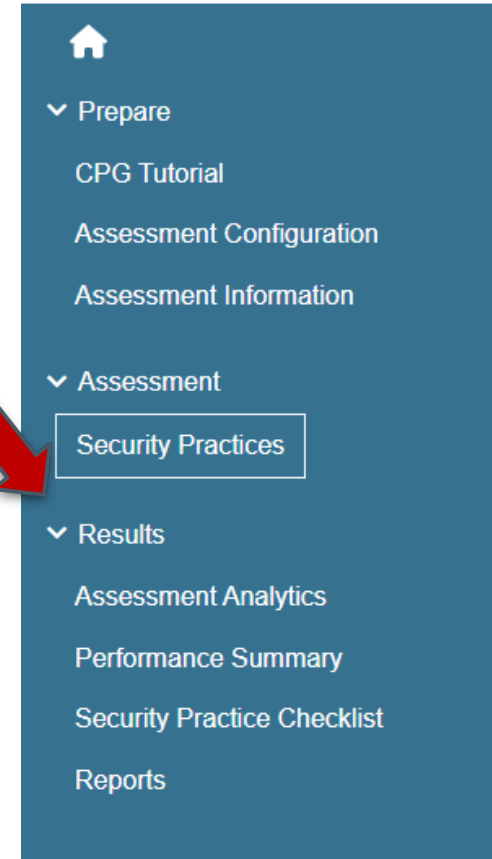
38/38

Security Practices - Cyber Performance Goals (CPG)

Select the applicable answer for each of the following questions. Unanswered questions are calculated as a 'Not' response.

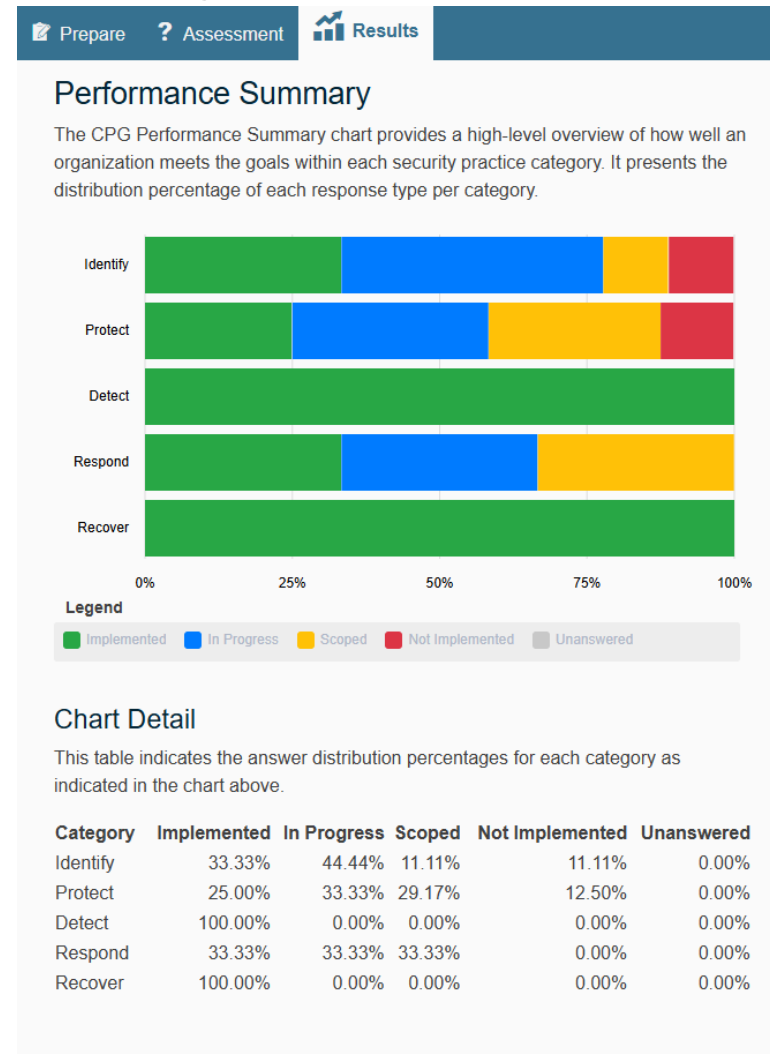
Identify	✓
Protect	✓
Detect	✓
Respond	✓
Recover	✓

Back Next



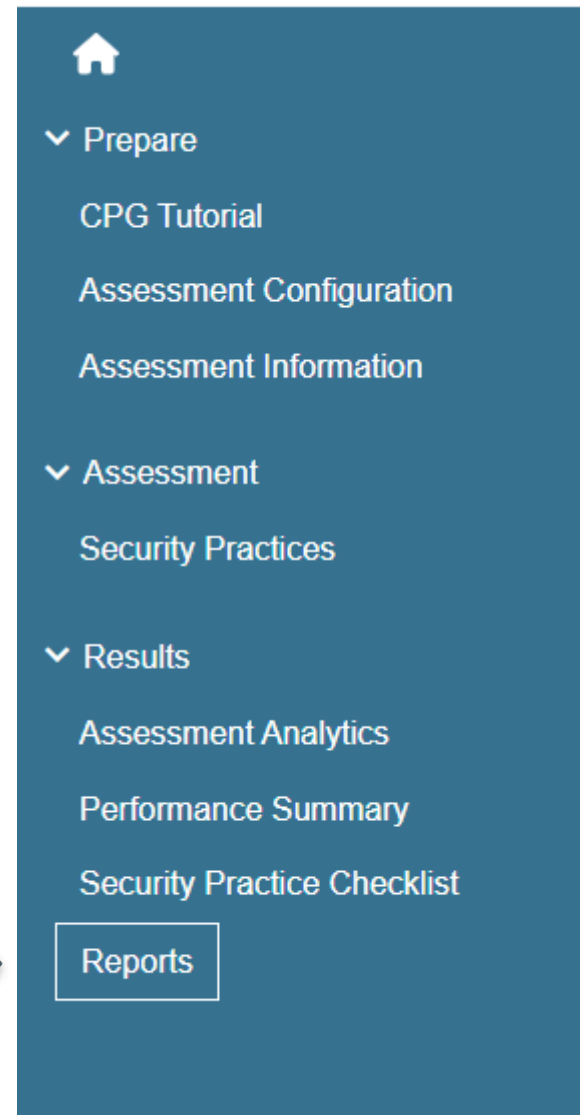
Performance Summary

- This slide shows an example of the Performance Summary section of the Results
- The “Chart Detail” corresponds to the information you will need to input in the Application and the Status Report in WebGrants annually, if awarded funding



CPG Report

- You will need to supply the CPG Report as an attachment to your Application and the Status Report in WebGrants annually, if awarded funding
- To access the report, select “Reports” on the left-hand side of the screen
- **Note: The CISA CPG Report contains sensitive cybersecurity information. This report is exempt from release under the Missouri Sunshine Law (Section 610.021 (19), RSMo).**



CPG Report

- Select “CPG Report”

Reports

Thank you for completing your assessment. The reports on this page capture summaries of your results that can help your organization’s cybersecurity planning and growth going forward. The assessment was last updated 2/18/2026, 11:29:37 AM GMT-0600. Any reports run prior to that update may not reflect the current state of the assessment.

[Printing Reports Instructions](#)

[Observations Tear-Out Sheets](#)

This report lists all Observations identified and recorded during the assessment. For more information, view the Observations Tear Out Sheets page in the User Guide.

[📄 Export Observations to Excel](#)

All Observations are exported to an Excel file. Observations assigned to multiple parties will have an entry for each person responsible.

Cross-Sector Cybersecurity Performance Goals (CPG)

[CPG Report](#)

The CPG Report includes the CPG Performance Summary and the Security Practice Checklist.



CPG Report

- The CPG Report will open in a new window
- Select “File” in the upper left-hand corner
- Select “Save as PDF”
- Select a location to save the file on your computer that will allow you to attach to the Application and the Status Report in WebGrants, if awarded funding



Questions

- For questions or assistance on the CISA CPG Assessment, contact the DPS/OHS Cybersecurity Team at the contact information below
 - Phone: 573-526-0153
 - Email: securityintel@mshp.dps.mo.gov

