CISA Cybersecurity Performance Goals (CPG) Assessment

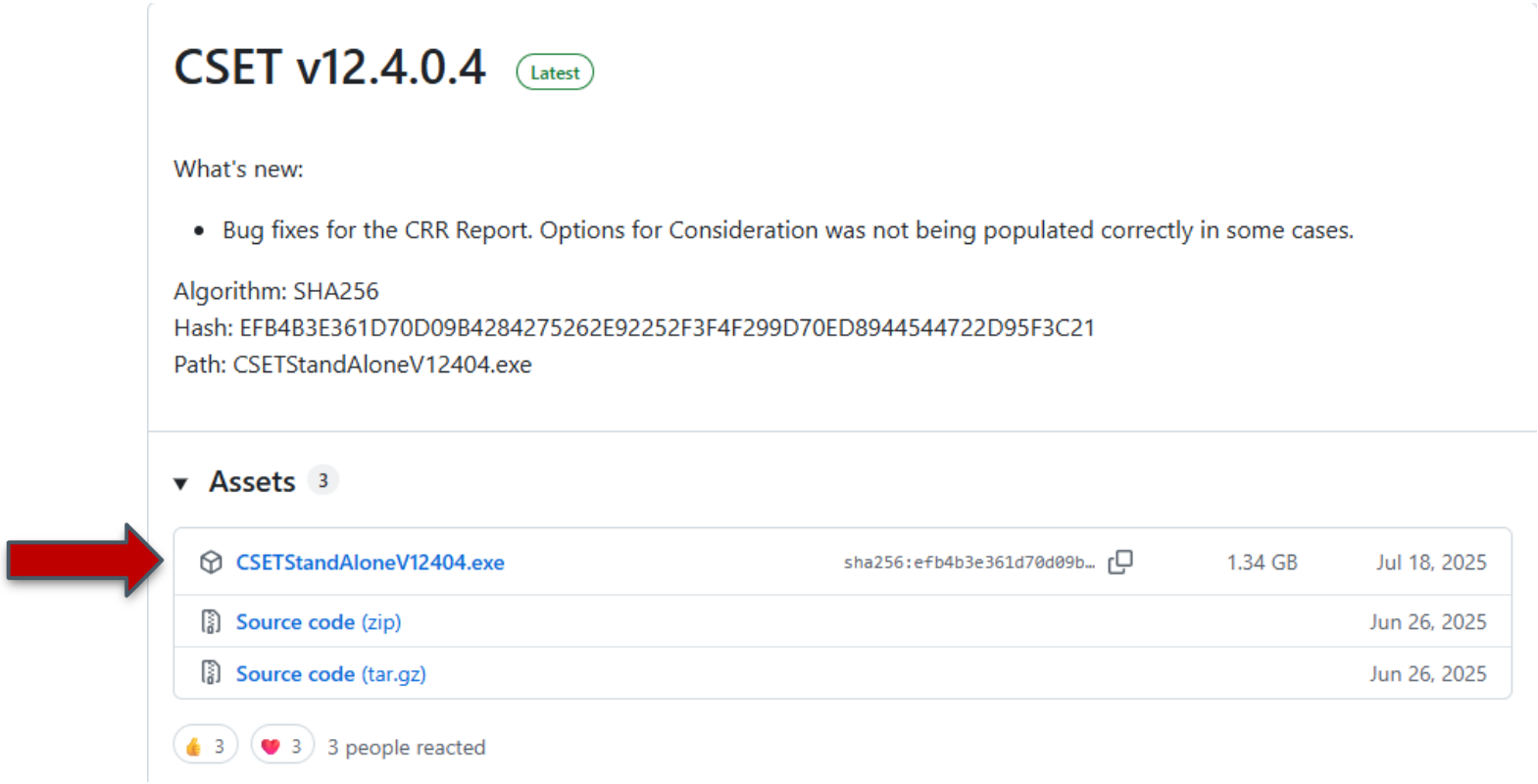
Missouri Department of Public Safety/Office of Homeland Security

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

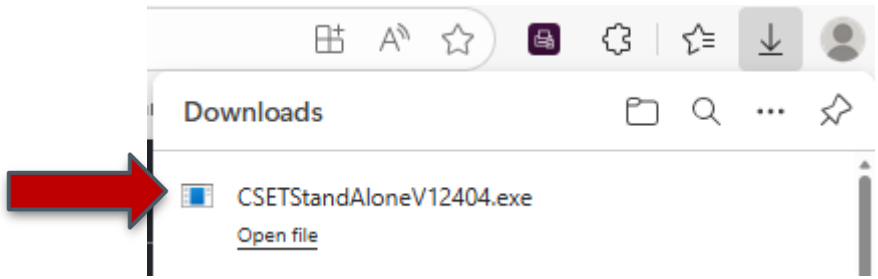
Download the CSET

- Under “Assets” select and download the CSET



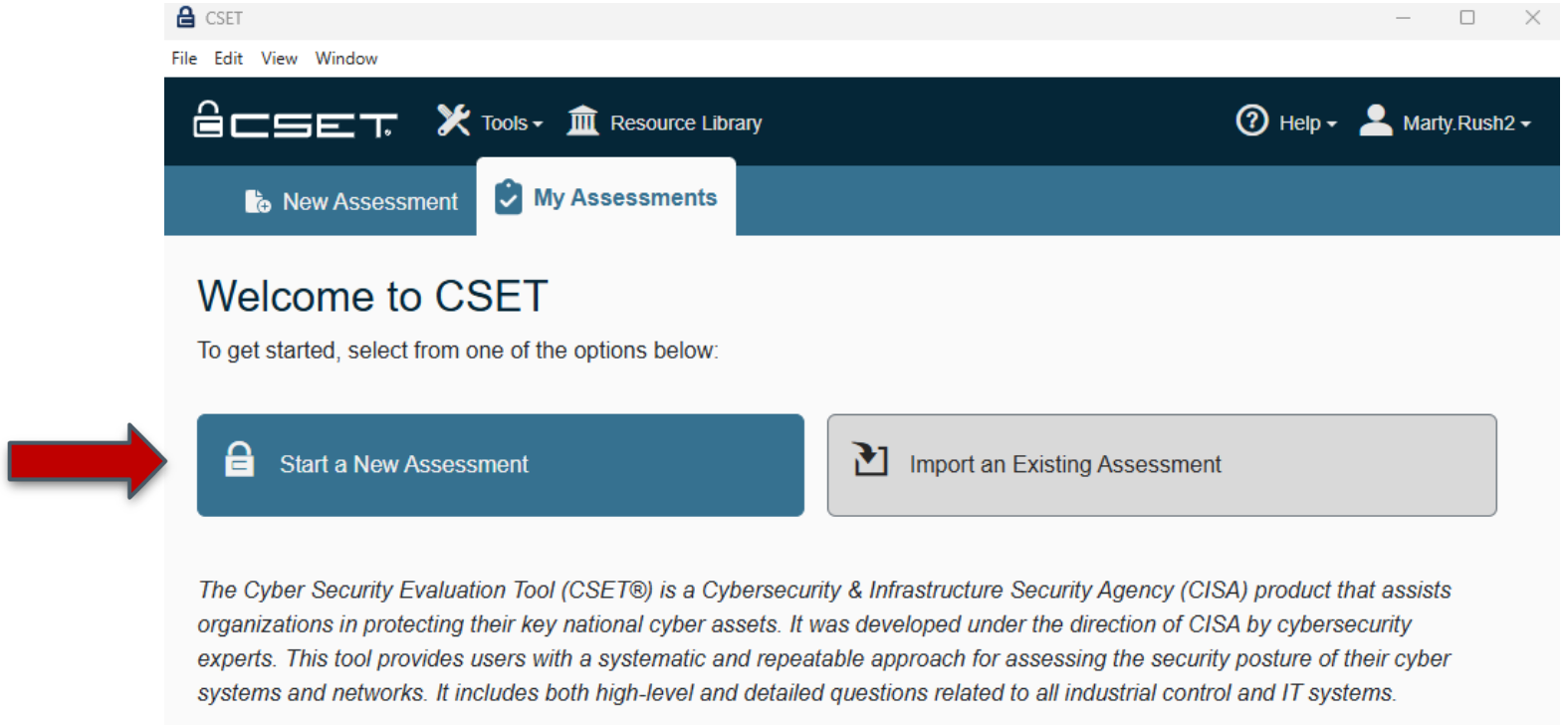
Download the CSET

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



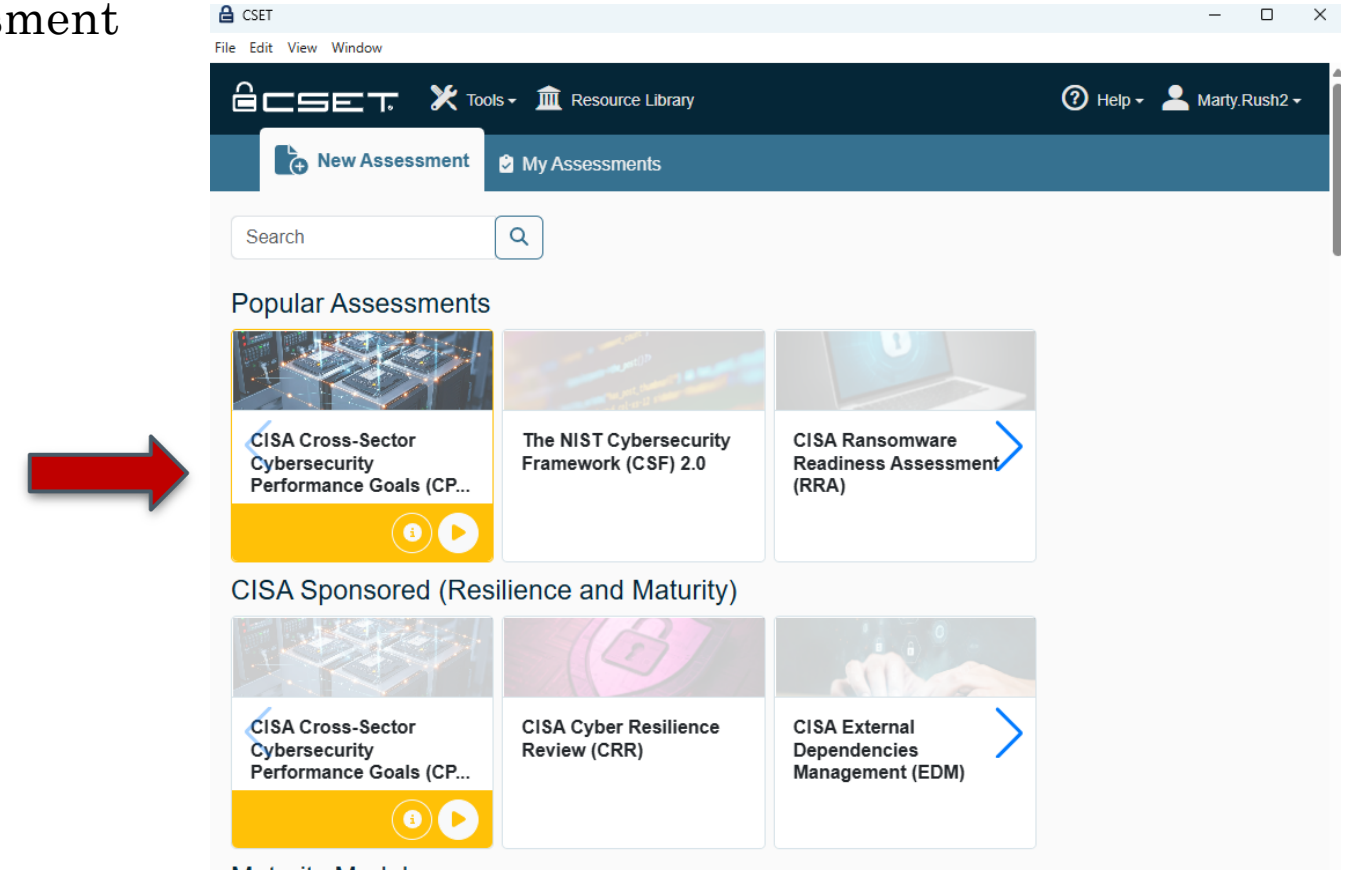
Starting an Assessment

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



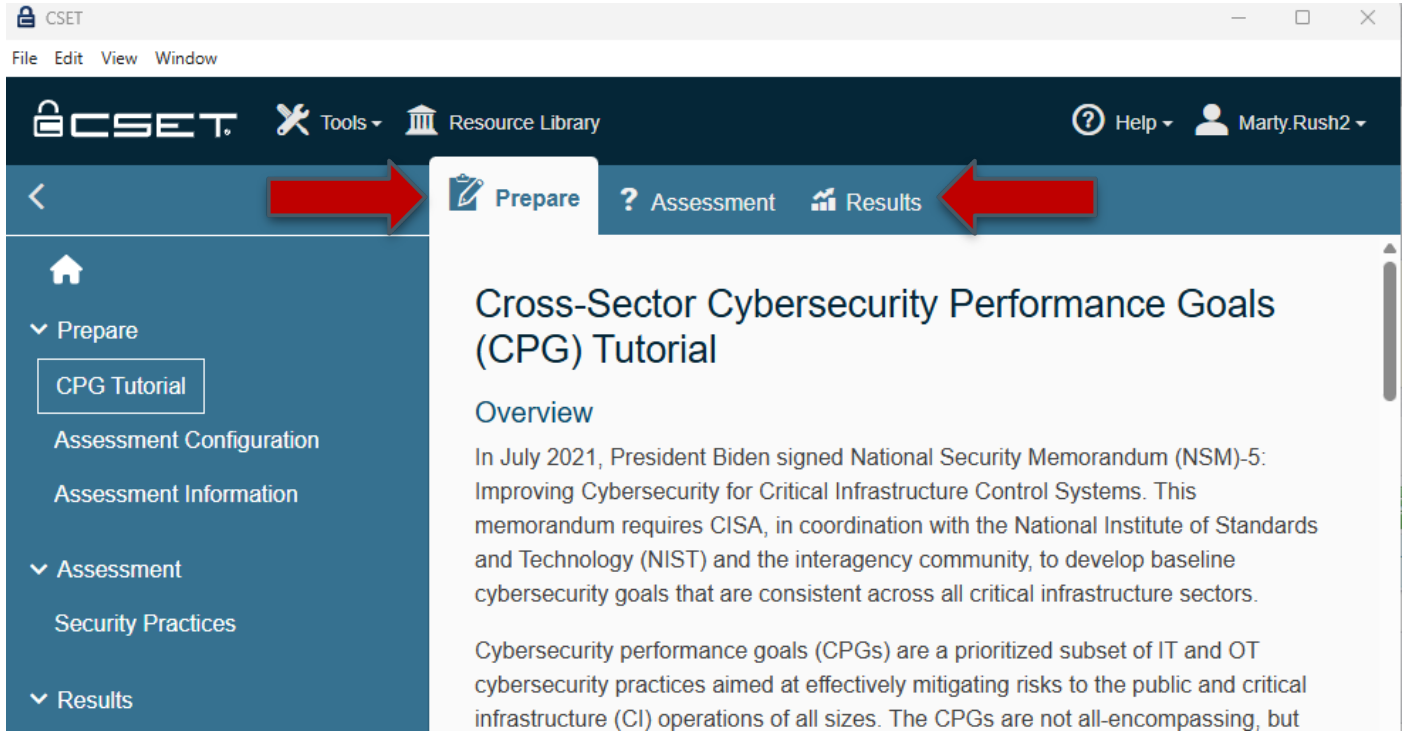
Starting an Assessment

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



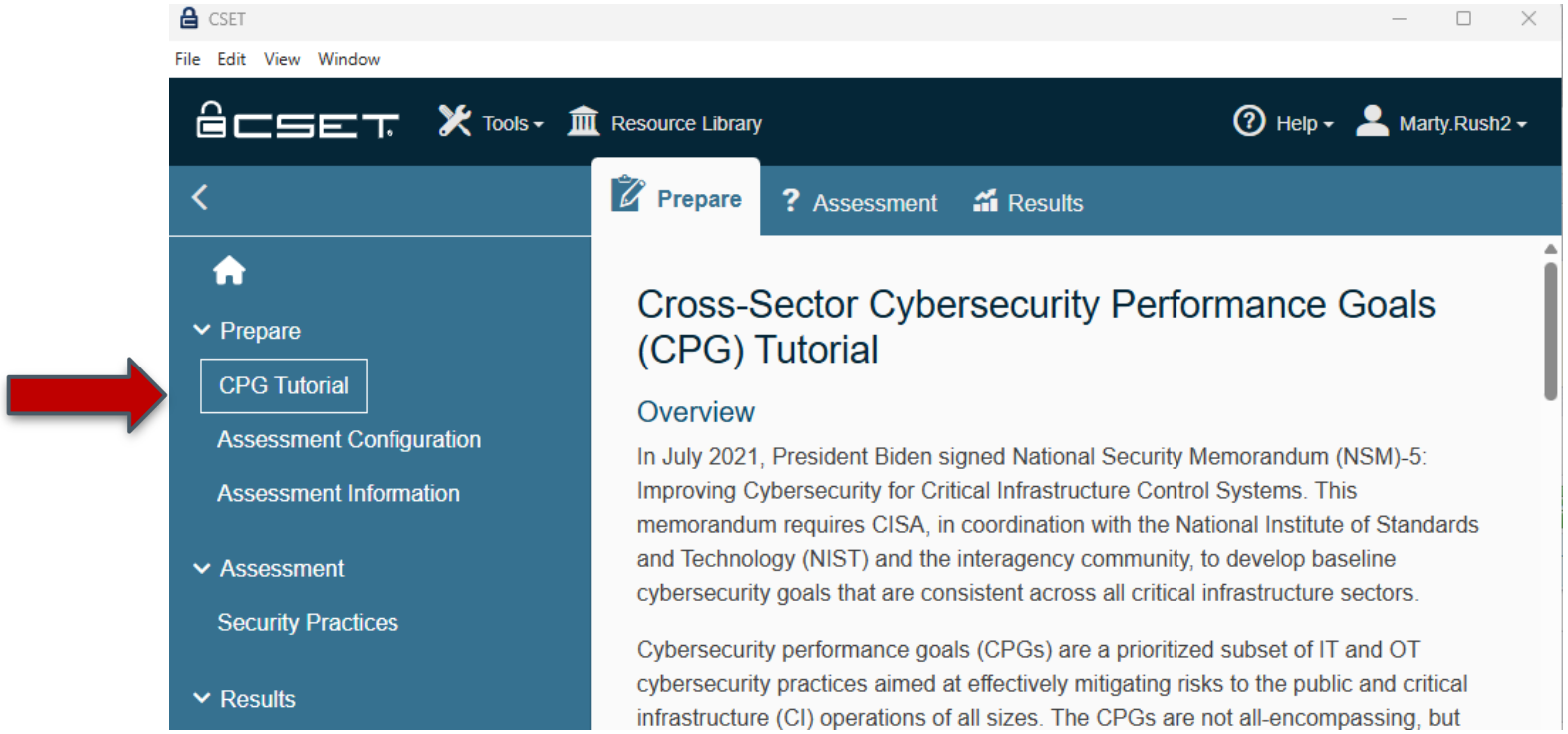
Assessment Overview

- 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



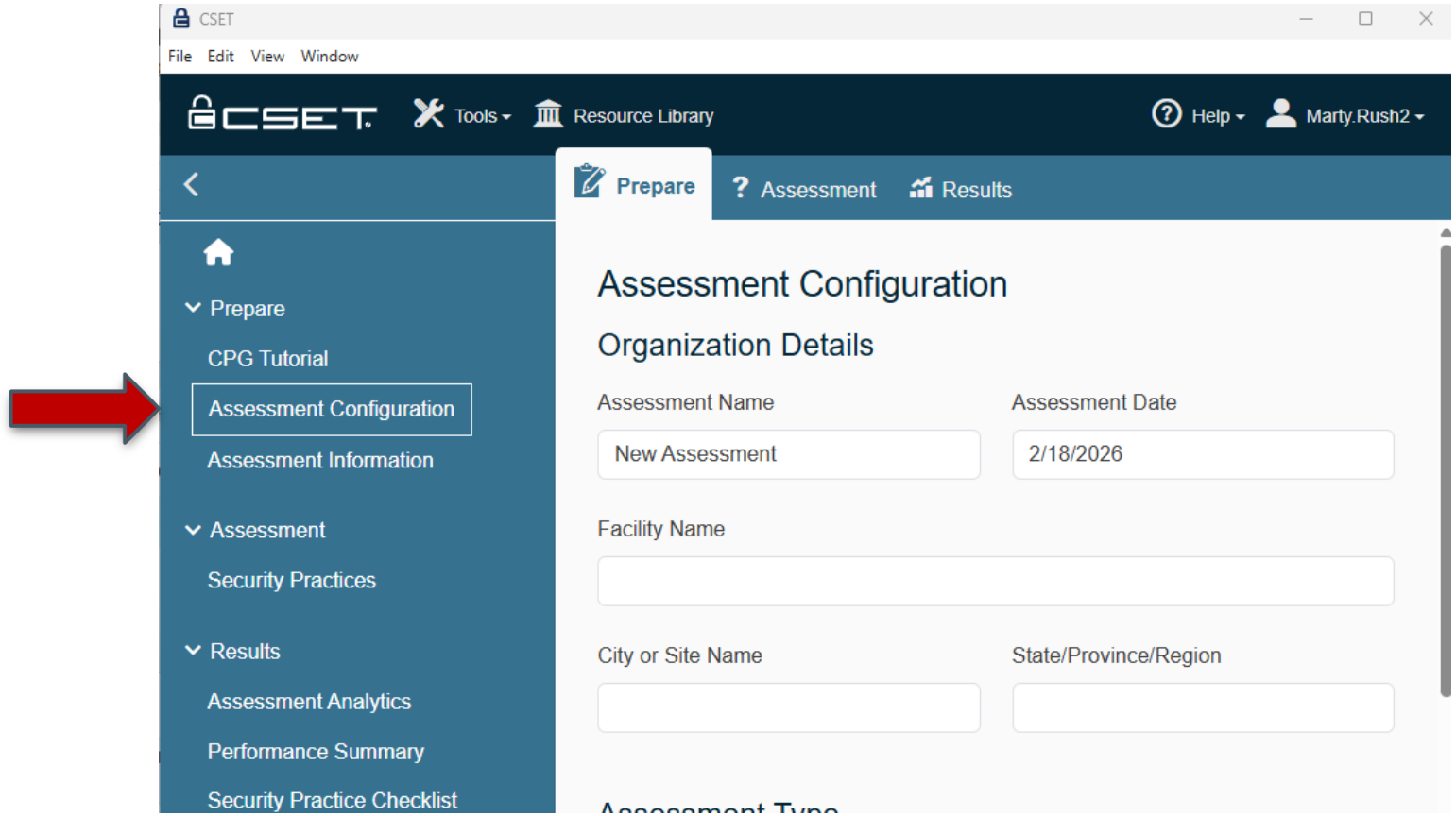
CPG Tutorial

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



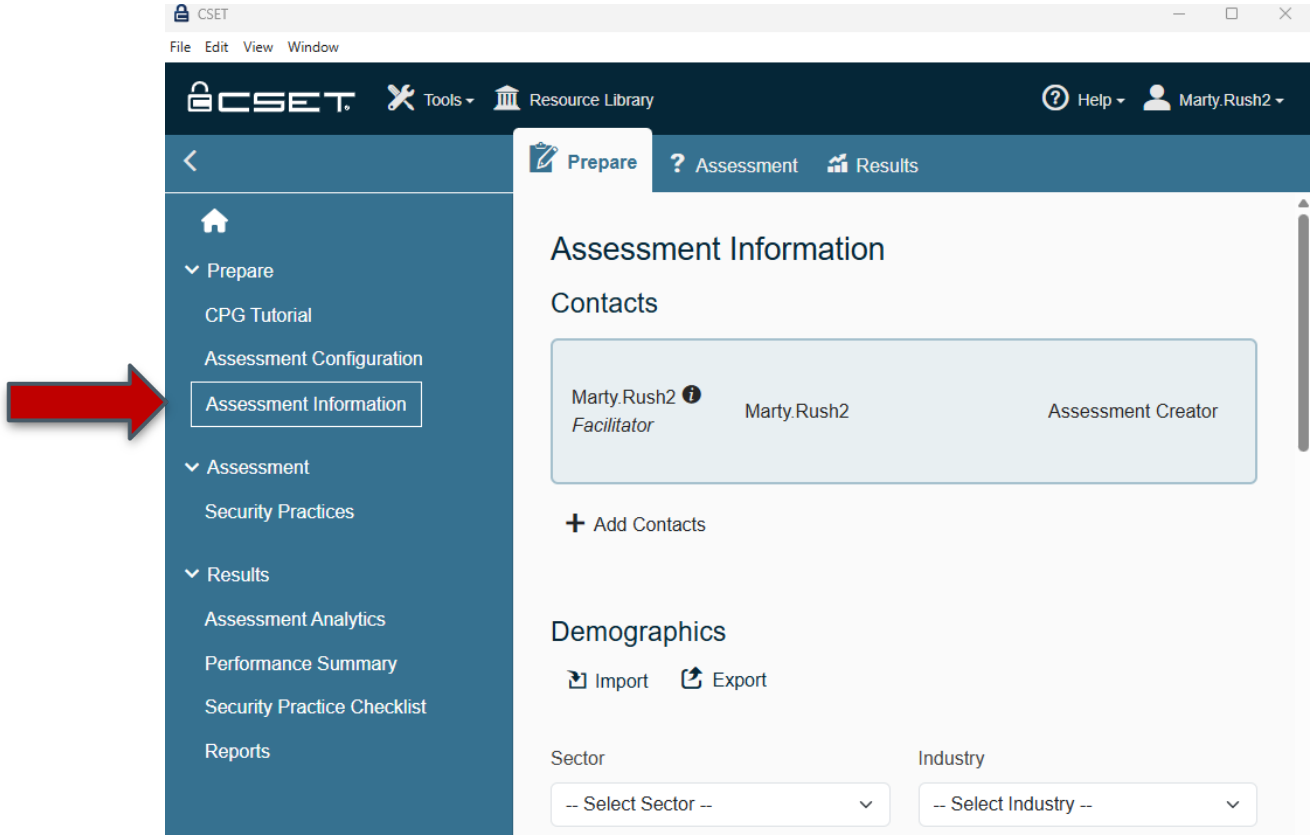
Assessment Configuration

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



Assessment Information

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



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

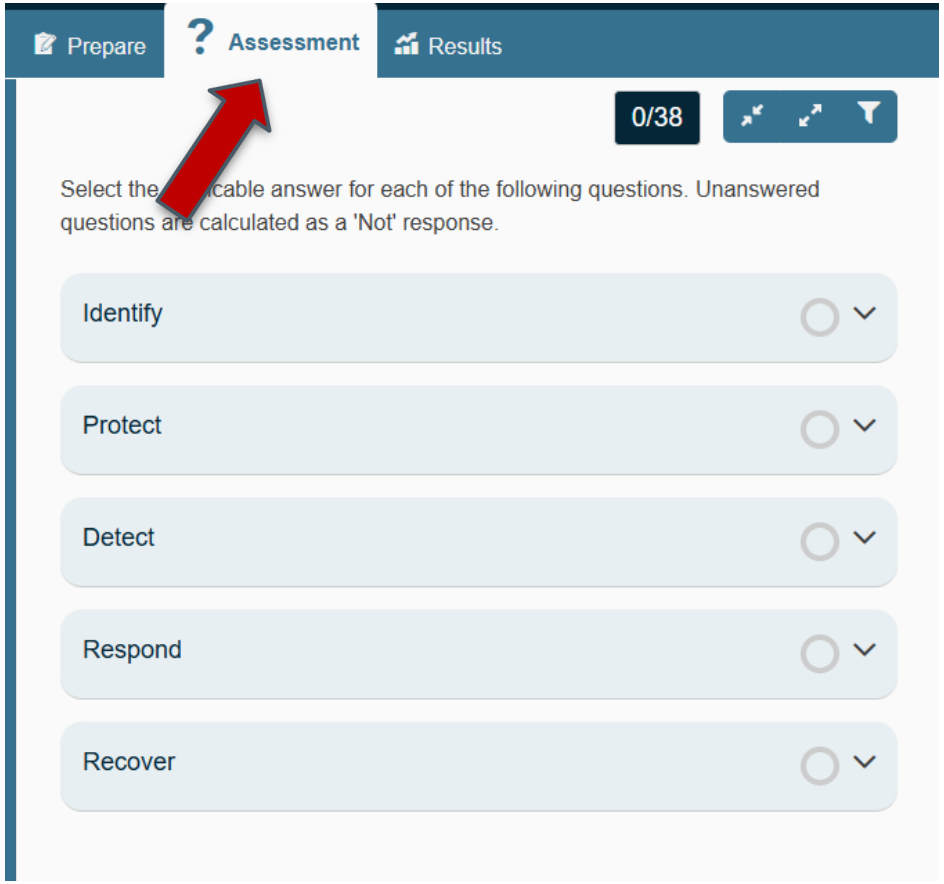
- Answer Buttons 

  - 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

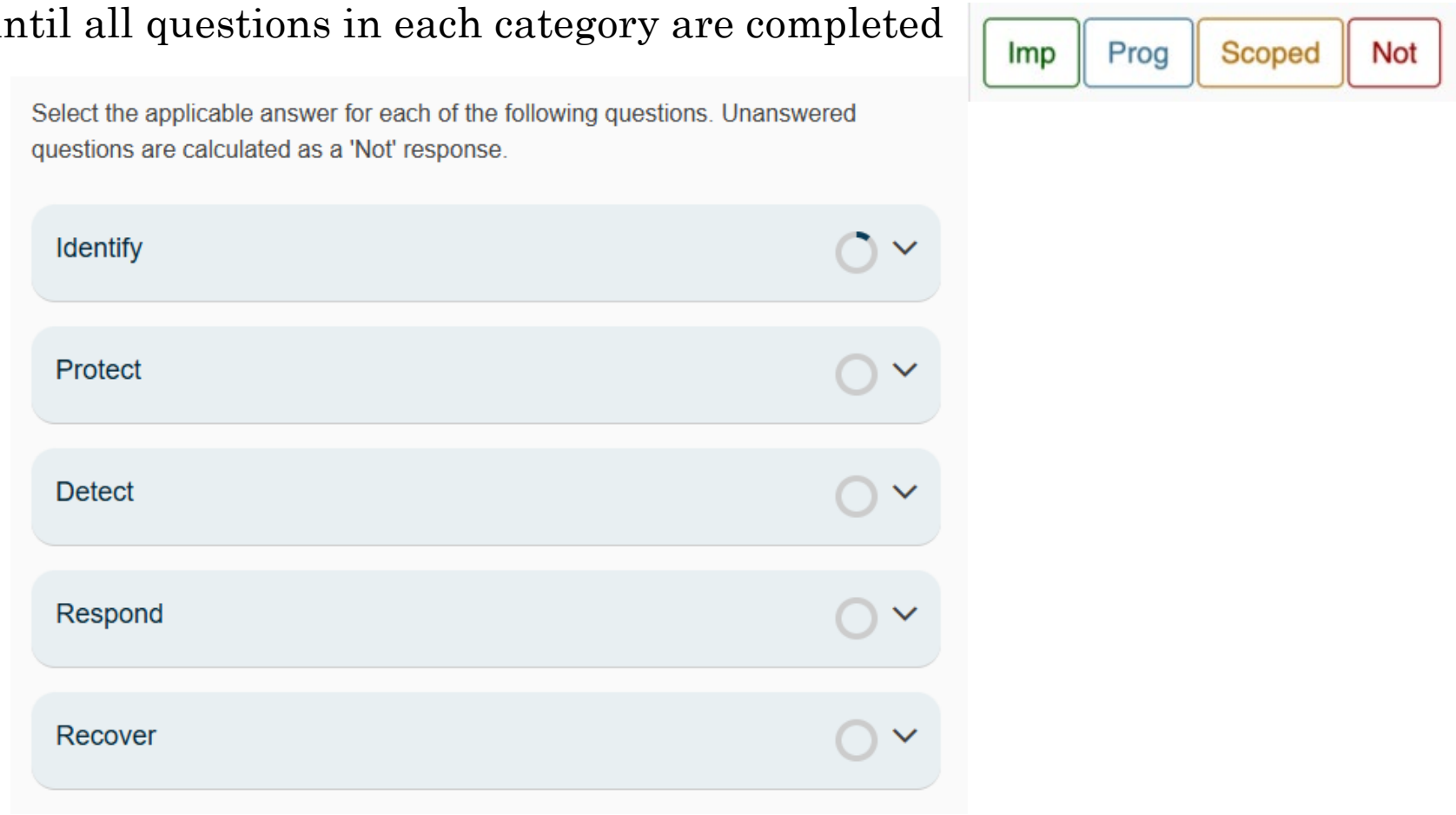
Assessment Completion

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



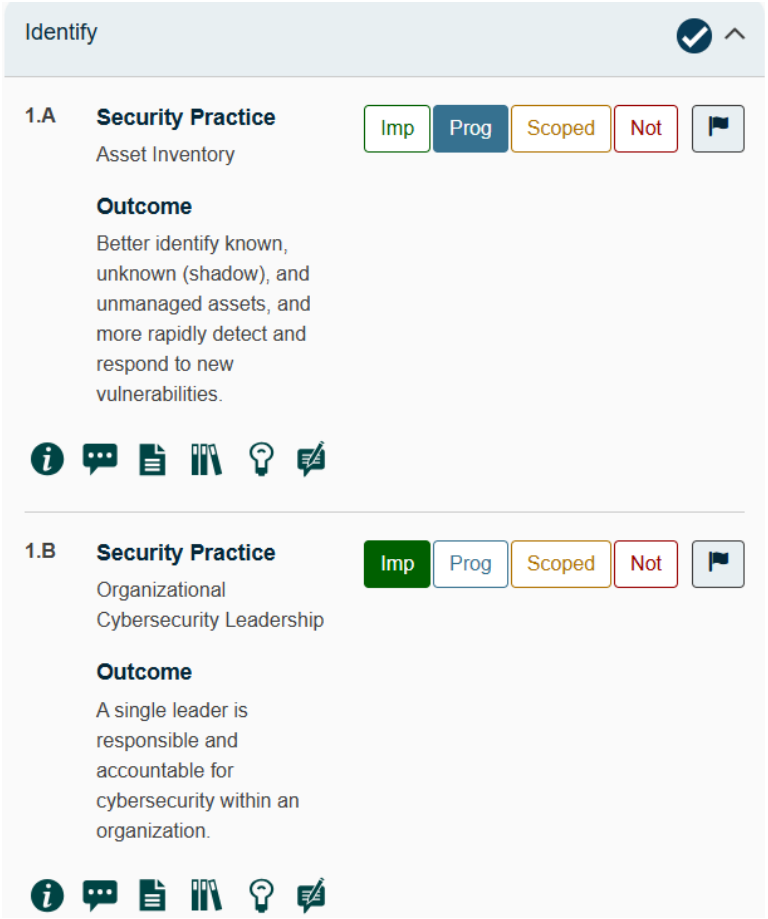
Assessment Completion

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



Assessment Completion

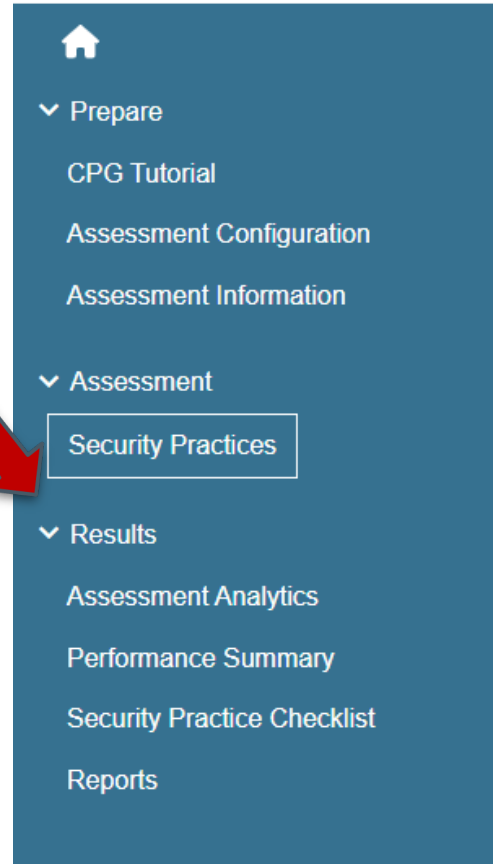
- Below is an example of the questions when you expand a NIST Category



Assessment Completion

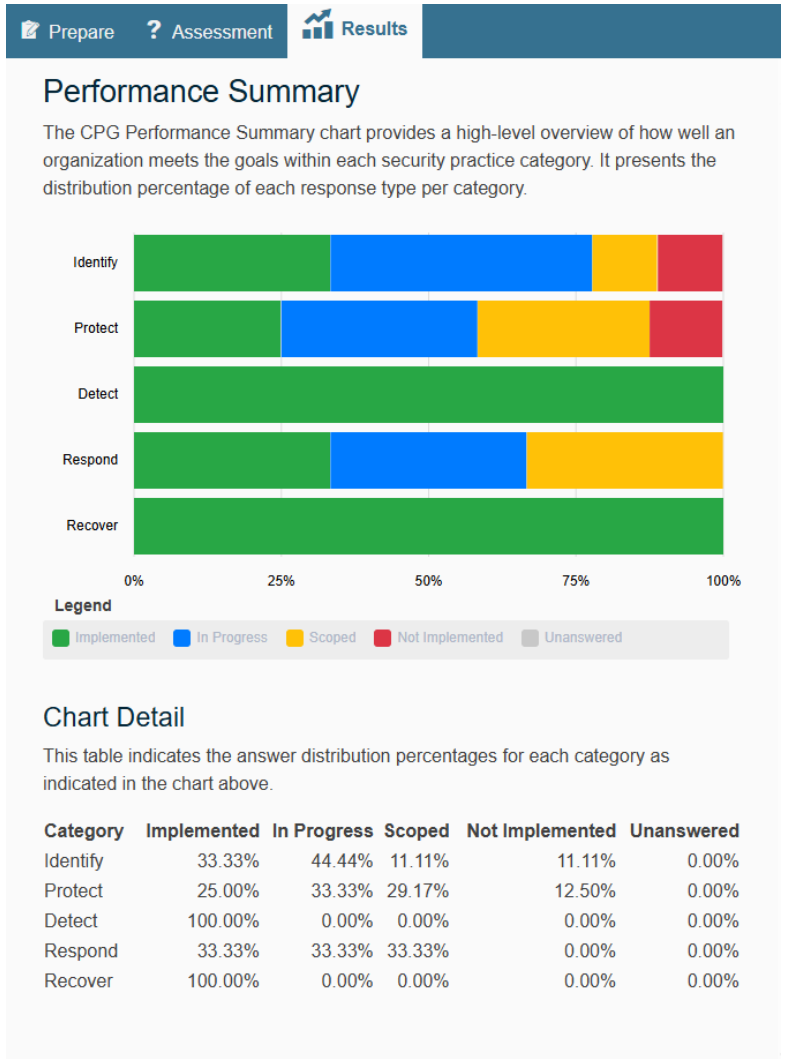
- After all questions have been answered, there are several options to review results:
  - Assessment Analytics
  - Performance Summary – the information contained in the Performance Summary will be submitted in your Application and the Status Report in WebGrants annually, if awarded funding
  - Security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



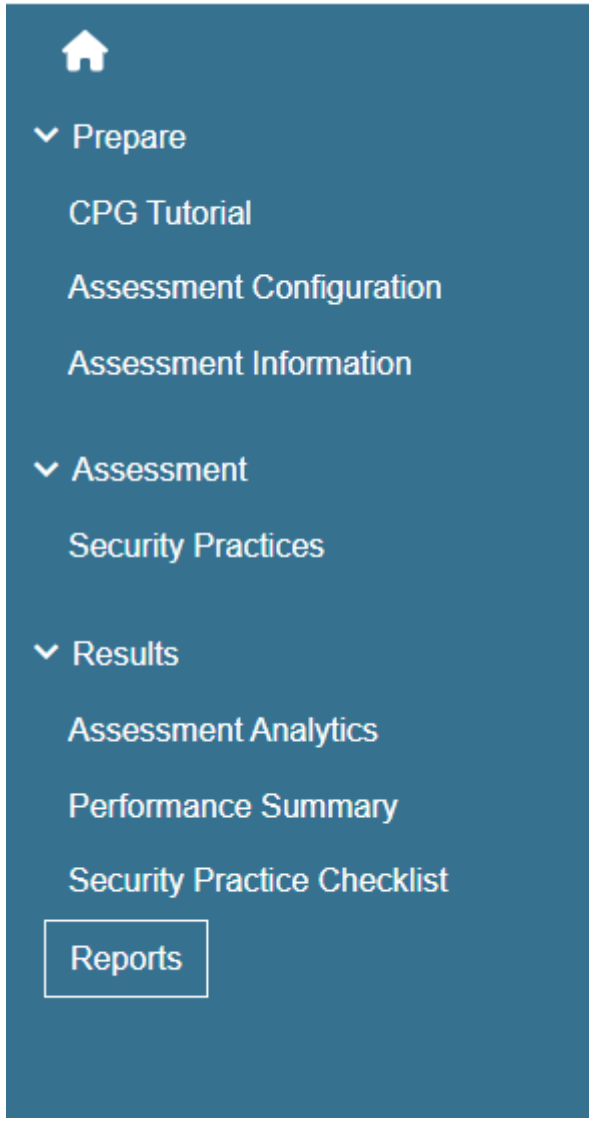
Performance Summary

- 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



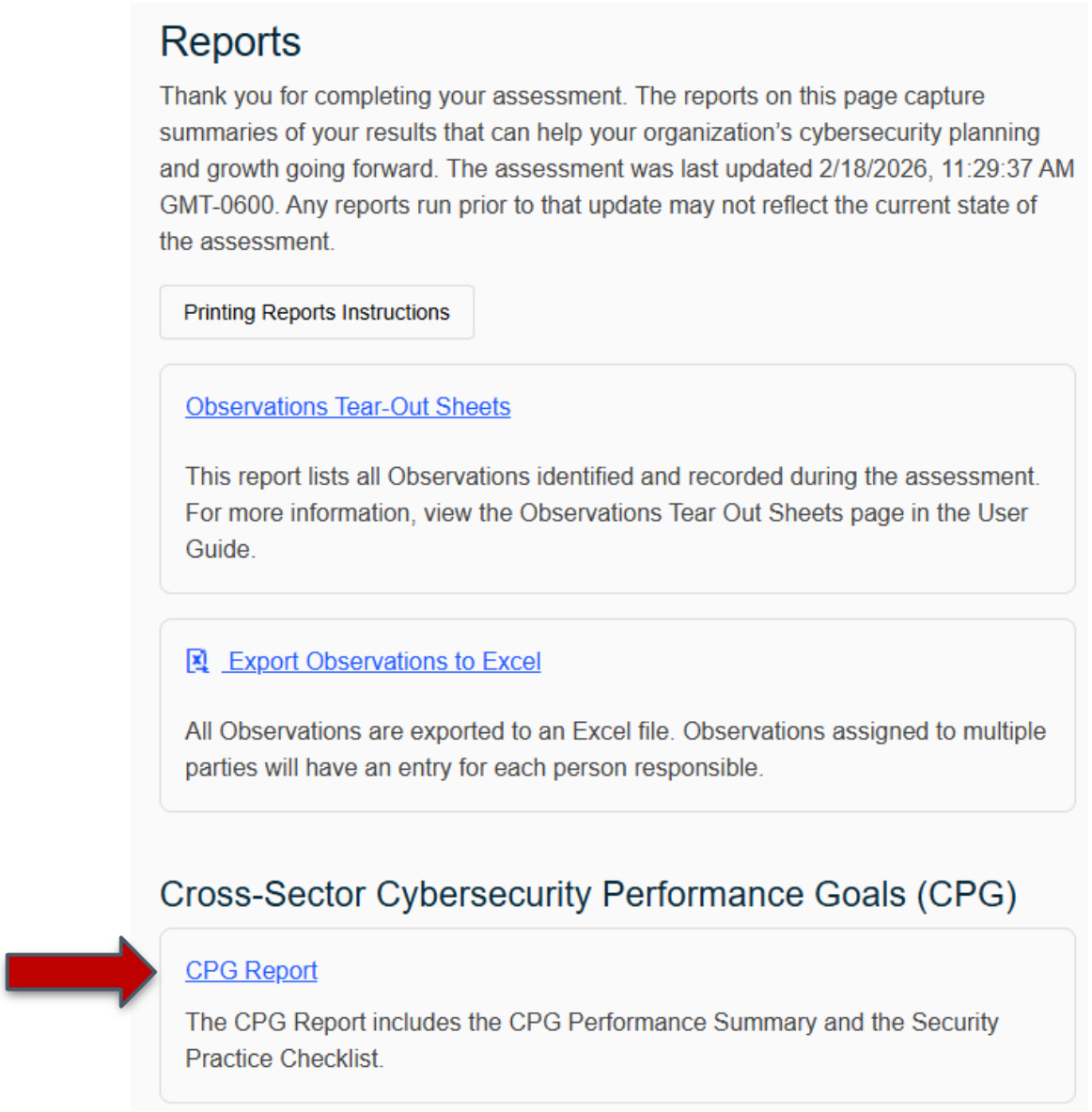
CPG Report

- 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”



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