WEB GUIDANCE TOOL USER GUIDE

Prepared for:

NCHRP Project 03-127
Cybersecurity of Traffic Management Systems

Prepared by:

Marisa C. Ramon
Ben A. Abbott, Ph. D
Austin T. Dodson
SOUTHWEST RESEARCH INSTITUTE®
Intelligent Systems Division
Post Office Drawer 28510, 6220 Culebra Road
San Antonio, Texas 78228-0510

(October, 2019)

The information contained in this report was prepared as part of NCHRP Project 03-127, National Cooperative Highway Research Program.

Acknowledgements (include in report)

This study was conducted with funding provided through the National Cooperative Highway Research Program (NCHRP) Project 03-127, *Cybersecurity of Traffic Management Systems.* The NCHRP is supported by annual voluntary contributions from the state Departments of Transportation. Project 03-127 is developing guidance for state and local transportation agencies on mitigating the risks from cyber-attacks on the field side of traffic management systems (including traffic signal systems, intelligent transportation systems, vehicle-to-infrastructure systems (V2I), and closed-circuit television systems) and, secondarily, on informing the agency's response to an attack. This document summarizes a variety of efforts applicable to the objective and will be updated throughout the life of the project. The report was prepared by Ben Abbott, Ph. D, Marisa Ramon, and Austin Dodson of the Southwest Research Institute. The work is being guided by a technical working group and managed by Ray Derr, NCHRP Senior Program Officer.

EXECUTIVE SUMMARY

As part of the Cyber-Attack Response Guidance Development phase of the research project, the research team has prepared a User Guide detailing the usage of the Traffic Management System (TMS) Cybersecurity Web Guidance Tool (WGT).

The WGT is a software application whose purpose is to aid a transportation agency to make its TMS field network more resistant to cybersecurity attacks. The WGT is not intended to replace the Risk Management process or be a complete cybersecurity assessment for an agency. Instead, its intention is to highlight areas for cybersecurity improvement and provide direction to improving one's cybersecurity posture.

The WGT will be web accessible through the National Operations Center of Excellence (NOCoE). The WGT is intended to be an easily understandable format to allow the end-user to privately and interactively complete a description of their field network devices to better understand their current security and receive suggestions to improve the security of their network.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

With more than 300,000 Traffic Signal Systems (TSS) across the United States and 2,550 added each year, based on the U.S. Census Bureau forecast of future population growth[1], Traffic Management Systems (TMS) have increasing cybersecurity risks. All these signalized systems contain varying levels of network access and embedded security. Traffic managers and government stakeholders may be unaware of the cybersecurity risks to field systems and other connected devices that relay data between systems and third parties or understand the likelihood of a cyber-attack occurring in one's network. Field systems and other connected devices introduce potential cybersecurity vulnerabilities that may be overlooked or not well understood by traffic managers and government agencies.

To help state and local agencies address cybersecurity risks on current transportation systems and those posed by integration of Connected and Automated Vehicles (CAV), Southwest Research Institute® (SwRI®) is currently researching cybersecurity weakness in TMS as part of program from the Transportation Research Board (TRB). The TRB is part of the private, nonprofit National Academies of Sciences, Engineering, and Medicine.

SwRI is leading the two-year project with support from Praetorian, and over the course of the program the team has conducted a security assessment of high-risk TMS and developed web-based guide to help transportation agencies safeguard their equipment.

1.1 Project Background

The objective of the overall research effort is to develop guidance for state and local transportation agencies for mitigating risks from cyber attacks and responding to cyber attacks on the field side of TMS (including traffic signal systems, intelligent transportation systems, Vehicle-To-Infrastructure systems (V2I), and closed-circuit television systems). The guidance will address the vulnerability of field equipment (e.g., traffic signal controller, changeable message signs, and V2I roadside units), field communications networks, and field-to-center communications. It will not address vulnerabilities within a traffic management center, within center-to-center communications, or insider risk (accidental or intentional).

The decision not to include traffic management centers within the scope of this project rests on the fact that the attack surface of a traffic management center is the same as a conventional network. Traffic management centers consist of devices such as workstations, servers, and network equipment, typically with Internet connectivity. The best practices to secure such environments are well understood, with multiple frameworks and guidelines being available to guide traffic management organizations. As such, the research team focused on addressing the best practices to secure traffic management field equipment.

1.2 Project Goals

The goal of this entire project is to improve the cybersecurity of TMS by:

- Performing a strategic literature review and investigation of ongoing security efforts
- Review state-of-the-art technologies across multiple disciplines

[1] https://www.access-board.gov/guidelines-and-standards/streets-sidewalks/144-public-rights-of-way-guidelines/regulatory-assessment

- Assess representative TMS and equipment
- Perform penetration testing on high-risk equipment
- Develop guidance for state and local agencies that aid in identifying:
    - Risks to their current field networks
    - Recommended changes they may implement to reduce those risks
    - Implications of the Connected Vehicle (CV) and Autonomous Vehicle (AV) technologies on the field networks
- Promote adoption and industry participation

This report is one of the several tasks performed under this project working toward the overall project objective.

1.3 Purpose of this Document

The purpose of the document is to detail the usage of the cybersecurity WGT. As a task of NCHRP 03-127, the WGT's purpose was to develop a cybersecurity guidance from a transportation business perspective, weighing in what factors impact safety and harm to people, customer privacy, damage to infrastructure, travel disruptions, and public perception that are important to the industry. By developing an understanding of industry problems, including integration of Connected and Automated Vehicles (CAV) technologies, and effectively modeling a TMS's cybersecurity risks, agencies can make system decisions, surrounding vendor procurement, network architecture and system implementation, and creating safer, more cyber-attack resilient TMS environments.

1.3.1 WGT Application Scope

The scope of the WGT effort is a web-based application providing technology agnostic results that can be utilized by end-users (i.e., state and municipal transportation agencies and vendors) for understanding and improving the cybersecurity posture of TMS-related technologies. The WGT allows users to identify relevant assets, conduct a self-assessment concerning security access controls and policies for both devices and networks, and provides a risk scoring based on a standard methodology that can be encrypted and saved locally and re-loaded for improvement comparisons over time.

1.4 Organization

This WGT user's guide consists of three (3) sections:

- *Introduction* - explains in general terms the overall project, the application purpose, and scope for which it is intended.
- *Application* Overview- provides a general overview of the application and its key features. The environment outlines the uses of the application's software requirements.
- *Application Use* - provides a detailed description of application functions, how information collected by the application is presented, and how to access the information.

2. APPLICATION OVERVIEW

The following sections describe the features and operating environment of the WGT.

2.1 Key Features

The WGT is composed of database files and web framework designed to make the risk modeling process more efficient. The following key features are implemented in the WGT:

- Designed to offer dynamic, user-driven information
- Analyzes data provided in the devices and questionnaire to find cybersecurity risk and report on findings in the form of Cybersecurity Risk reports
- Provides historical information by time stamping all reports generated
- Allows importing of questionnaire data
- Allows the user to create and manage a database through the admin portal
- Provides flexibility and expandability using a Model-View-Controller (MVC) development approach

2.2 Environment

The WGT was developed and tested primarily using Firefox version 65.0.1 web browser and on a MACOS operating system. While the WGT site was also tested using Internet Explorer 11, Microsoft Edge 44.X, and Chrome, there are some sections of the site that may not look correct using these browsers, but the program still functions correctly.

The software requirements for operating the WGT on a server are as follows:

- Python version 2.7.X
- PostgreSQL version 9.4
- Django version 1.11.15
- django-admin-sortable version 2.1.7
- et-xmlfile version 1.0.1
- jdcal version 1.4
- nltk version 3.3
- openpyxl version 2.5.5
- pyasn1 version 0.4.4
- pycrypto version 2.6.1
- python-keyczar version 0.716
- pytz version 2018.5
- six version 1.11.0

2.3 System Operations

The WGT operates on computers of all operating systems, with at least 2GB of Random Access Memory (RAM) allocated to the Operating System (OS), and enough disk space to accommodate the size of the database. To gain useful results, it is recommended that a user has a good working knowledge of the processes and procedures followed in their TMS. The application is accessed through a web browser at the address *cyberguidance.transportationops.org*, so a connection to the Internet is required to use the application. Also, if the software requirements are not met, Internet access may be needed to download

and install the necessary libraries. The user may download the application results as an encrypted data file or print to a PDF file for offline viewing. The overall system is shown in Figure 1.

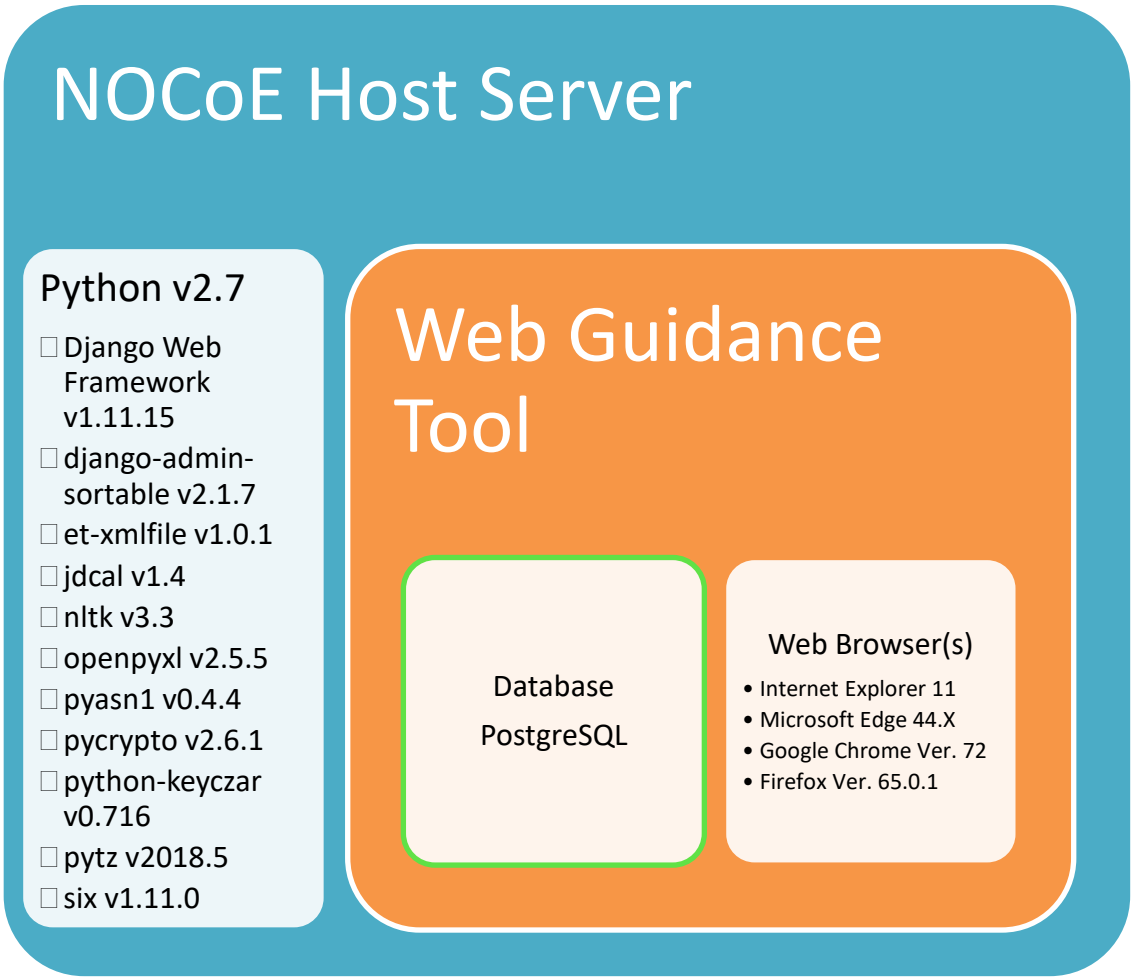

Figure 1. Web Guidance Tool Application Organization

3. APPLICATION USE

The following sections describe the procedures for using the application.

3.1 Instructions

Open a browser to the address: https://cyberguidance.transportationops.org

The WGT login page should appear as shown in Figure 2.

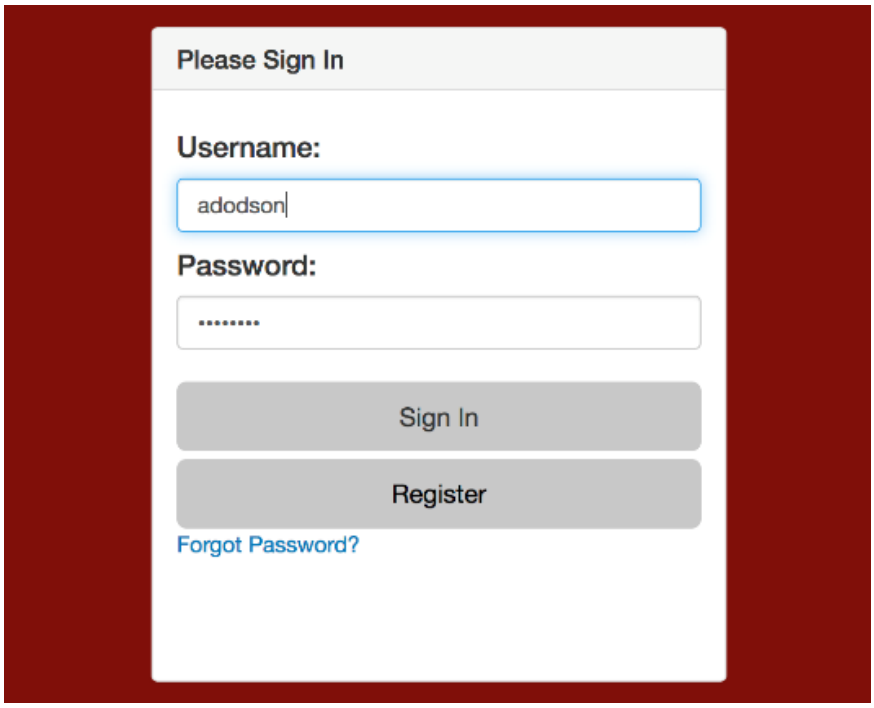

Figure 2. WGT Login Page

The end-user will have to register and create a login account to use the site, shown in Figure 3. Registration will require the user to input a username, email, password, and a user role that will determine what questions they will be presented with later in the WGT. If a user wishes to change their password after registering, they will need to follow the steps outlined in Section 3.2.1.

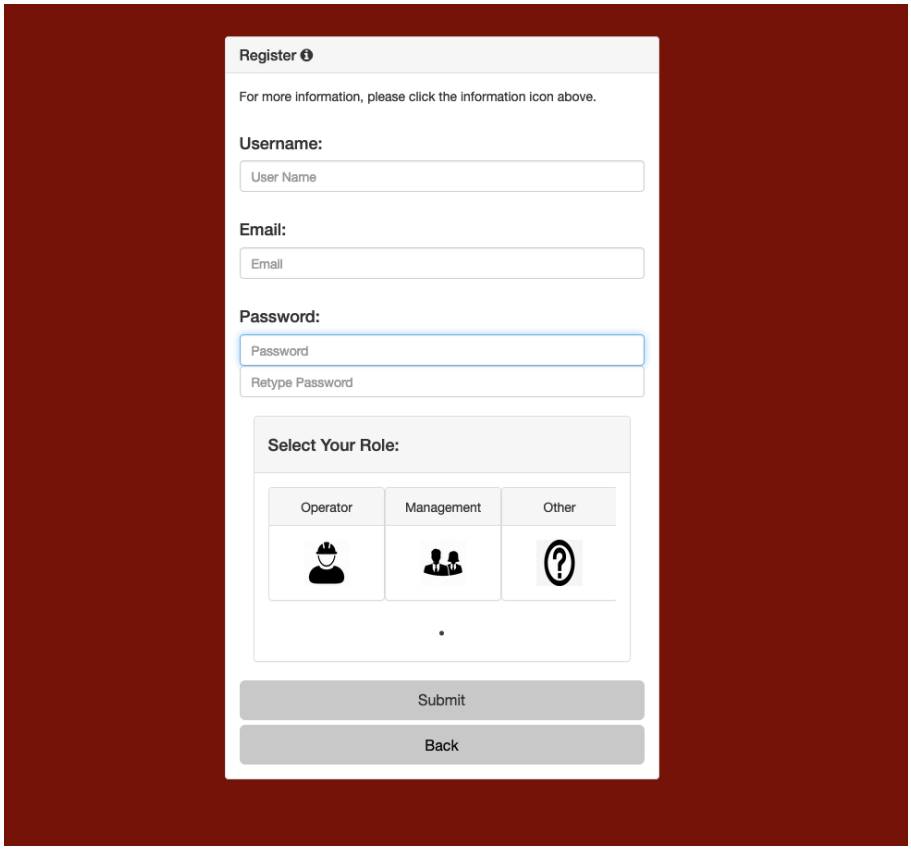

Figure 3. WGT Registration Page

Once the user types in their username and password and clicks Sign In, the WGT Main page should appear as shown in Figure 4. Included on this page are three main sections, the first is titled “TRB Risk Assessment Web Tool”, and looks to describe the process of the WGT to the user. Next is a section titled “User Info”, which includes information such as the username of the currently logged in user, the last time the user accessed the WGT, and the current role selected by the user. Finally, in the “Returning User” section, if a user has previously completed the WGT, they will be able to upload their user information file received by completing the WGT to view their previous results easily.

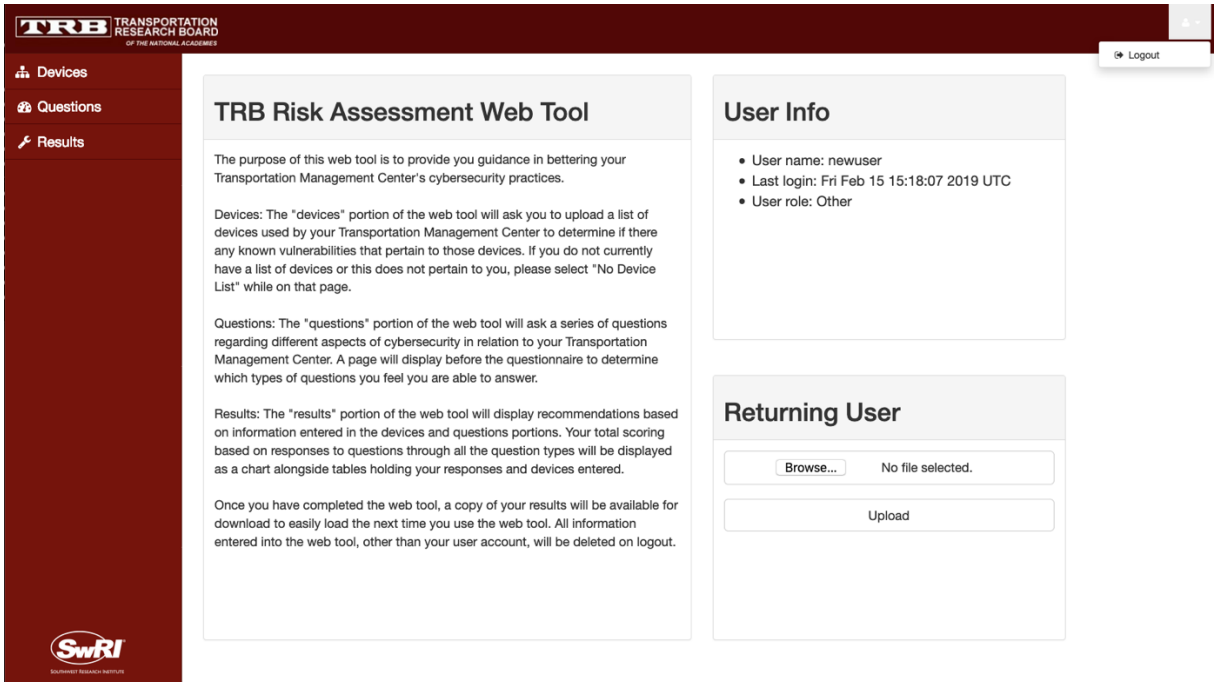

Figure 4. WGT Landing Page

3.1.1 Taking the Risk Assessment

The following sub-sections discuss the process for taking the cybersecurity risk self-assessment. The risk assessment is composed of three parts. The first two parts are inputs and include the selection of devices present in the user's environment and a security questionnaire asking about security policies and controls in place for both the devices and the network. Note that many of the questions relate to a TMS using a local network and may not apply to a TMS that is using only serial communication to communicate to field devices. The third part is the output from the two (2) inputs, the results page can then perform a high-level risk assessment of the user's environment and provide recommendations. These parts are shown as links on the left side of the main page as shown in in Figure 4.

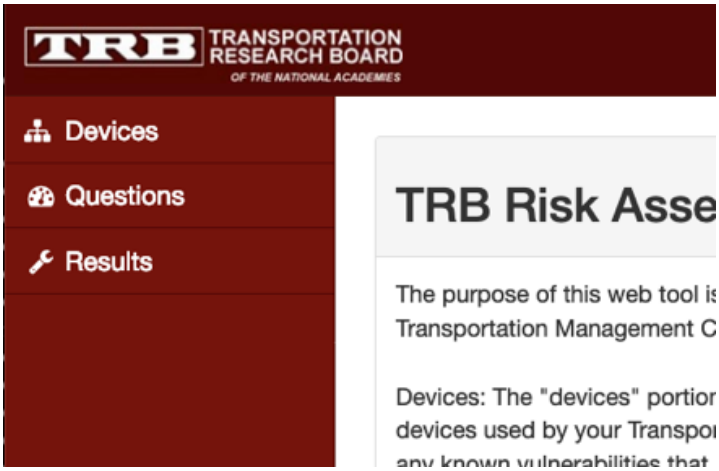

Figure 5. WGT three parts of the risk assessment

3.1.1.1 Selecting Applicable Devices

To begin the risk assessment, the end-user must select the devices that are present in their environment as shown in Figure 6. This will allow the guidance to provide best practices concerning the devices in the environment.

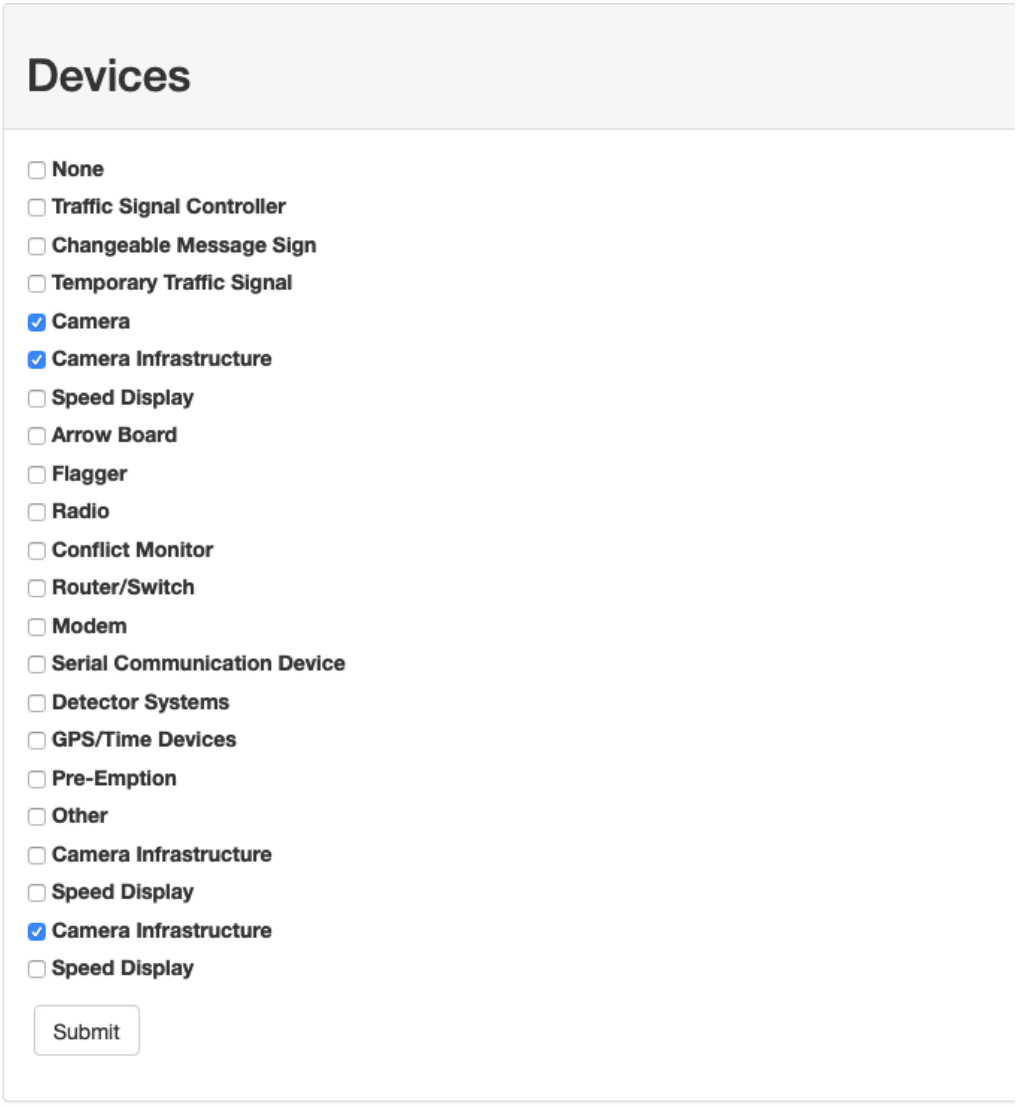

Figure 6. WGT - Cyber Guidance Devices Selection

The categories of devices listed on the Devices page are drawn from the set of devices outlined in Task 2 of the effort. These device types were accumulated from state Department of Transportation (DOT) public facing sites, and then filtered into the devices that could affect driving conditions or the larger TMS. Examples of the risks that these devices present include but are not limited to worsening traffic conditions, causing harm to pedestrians, and causing TMS communication disruptions. For each of these device types, there is an associated recommendation. An example of a recommendation for the "Traffic Signal Controller" section is to limit the access of open networking ports to authorized users.

3.1.1.2 Filling out the Questionnaire

After selecting the application devices, the user will next select the questionnaire link to begin a self-assessment of their security policies, access controls, and practices implemented, as shown in Figure 7. This questionnaire consists of 102 questions, but the number of questions presented to the user will vary based on the user's role and answers to certain questions. Estimated duration of the questionnaire is approximately 30 minutes. To begin the questionnaire, the user must first select question groups they feel are applicable to their position. The presented question groups, shown in Figure 8, are based on the user's role. These groups, and the questions in the groups by extension, are gathered from the standard NIST 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations". Each of the groups can be defined as follows:

- Access Control – This group contains questions pertaining to has a user will access the TMS.
- Audit and Accountability – This group contains questions that assess the documenting and traceability of procedures used by a TMS.
- Security Assessment – This group contains questions that determine if the security-based testing completed by a TMS is adequate.
- Identification and Authentication – This group contains questions that review the security functions in place to check that a user is supposed to be using the TMS.
- Physical and Environmental Protection – This group contains questions that assess the physical (barriers, walls, etc) security procedures implemented by a TMS.
- Personnel Security – This group contains questions that address purpose, roles, management commitment, and coordination among transportation entities, and compliance.

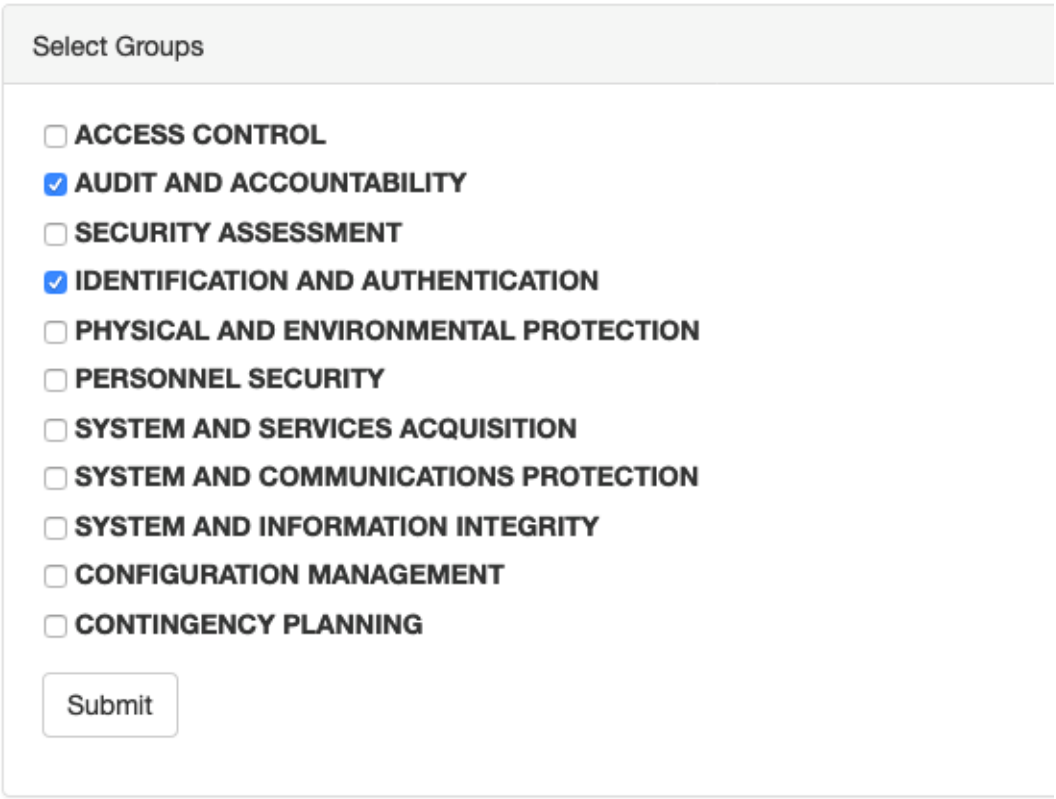

Figure 7. WGT - Question Group Selection

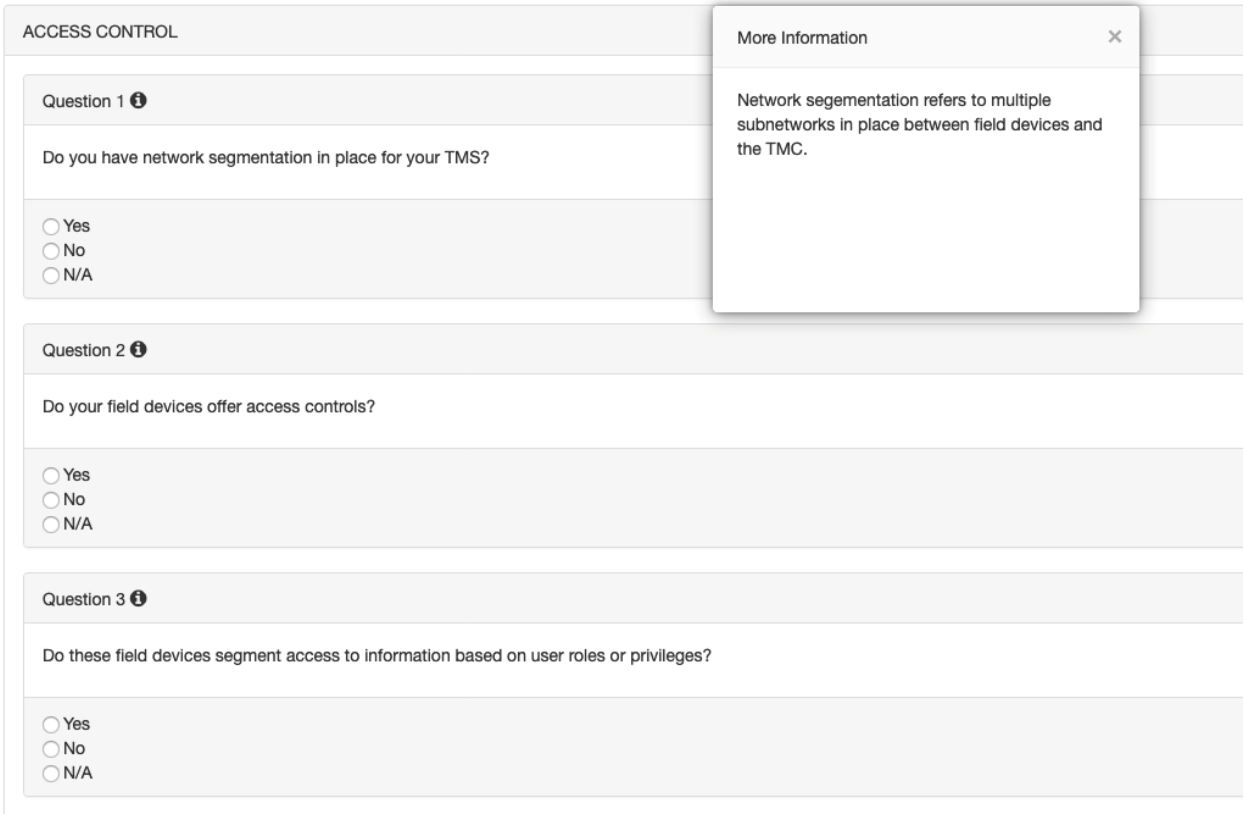

Figure 8. WGT - Cyber Guidance Questionnaire

The questionnaire is presented to the user based on which groups they selected. Each question is formatted to include the question number, the question itself, and choices for the response. Also, each question contains a more information icon represented by a "i". These can be clicked to display information to help the user better understand the question. A sample question asked by the questionnaire in the "Access Control" section is "Do you have network segmentation in place for your TMS?", and a user can choose a listed response to answer the question: "Yes", "No", or "N/A".

3.1.2 Viewing the Results

After selecting the application devices and answering the risk assessment questionnaire, the results of the cybersecurity risk assessment will be displayed on the Risk Results Report page.

3.1.2.1 Cyber Guidance Results Summary Report

Upon clicking on the 'Results' link, your page will look similar to the screen shown in Figure 9.

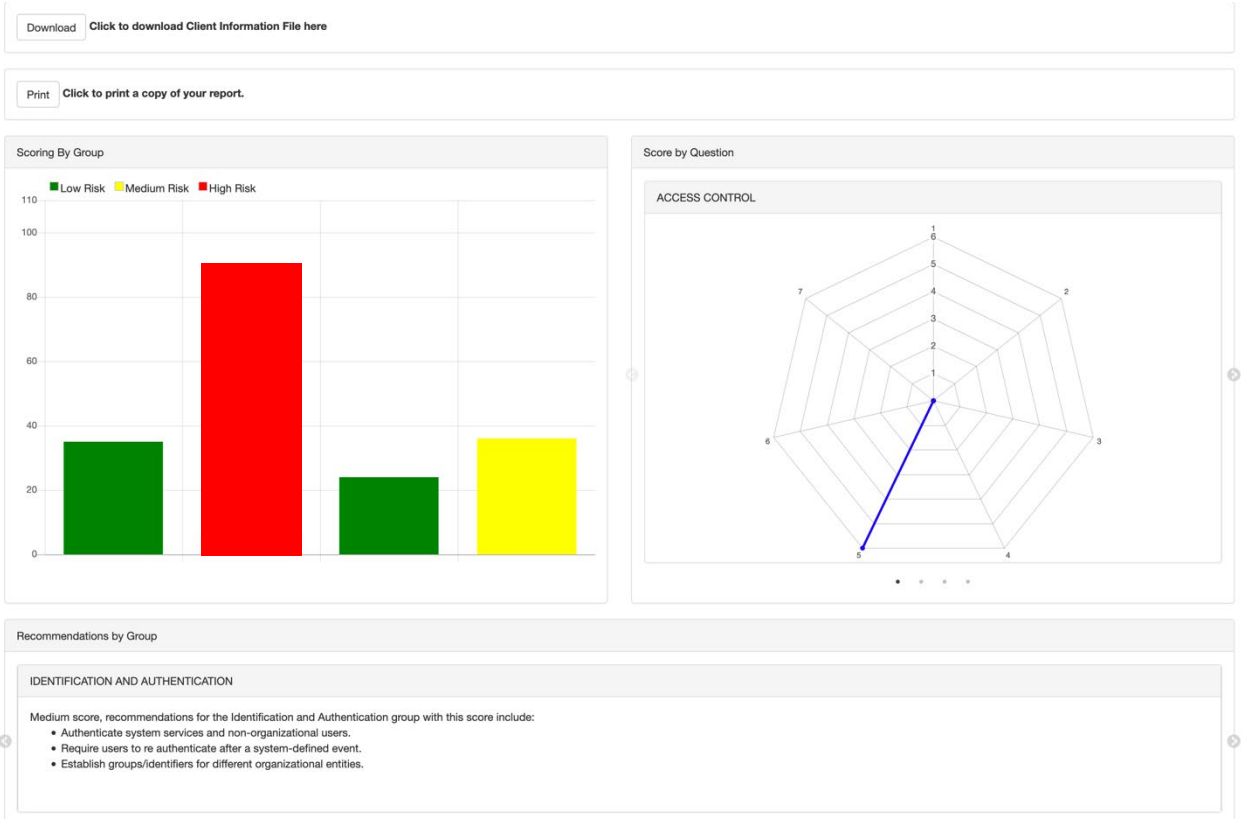

Figure 9. WGT - Cyber Guidance Results Summary Report – Part 1

The Cyber Guidance Results Summary Report, shown in Figure 10, will present an overview of the TMS's risk analysis including a risk scoring, selected devices, answers to the risk assessment questionnaire, the risk formula used for the calculation, and recommendations to improve the TMS's security posture.

The Results pages consist of the following sections:

- Results Download
- Print Report
- Scoring by Group
- Scoring by Question
- Recommendations by Group
- Risk Assessment Responses Review

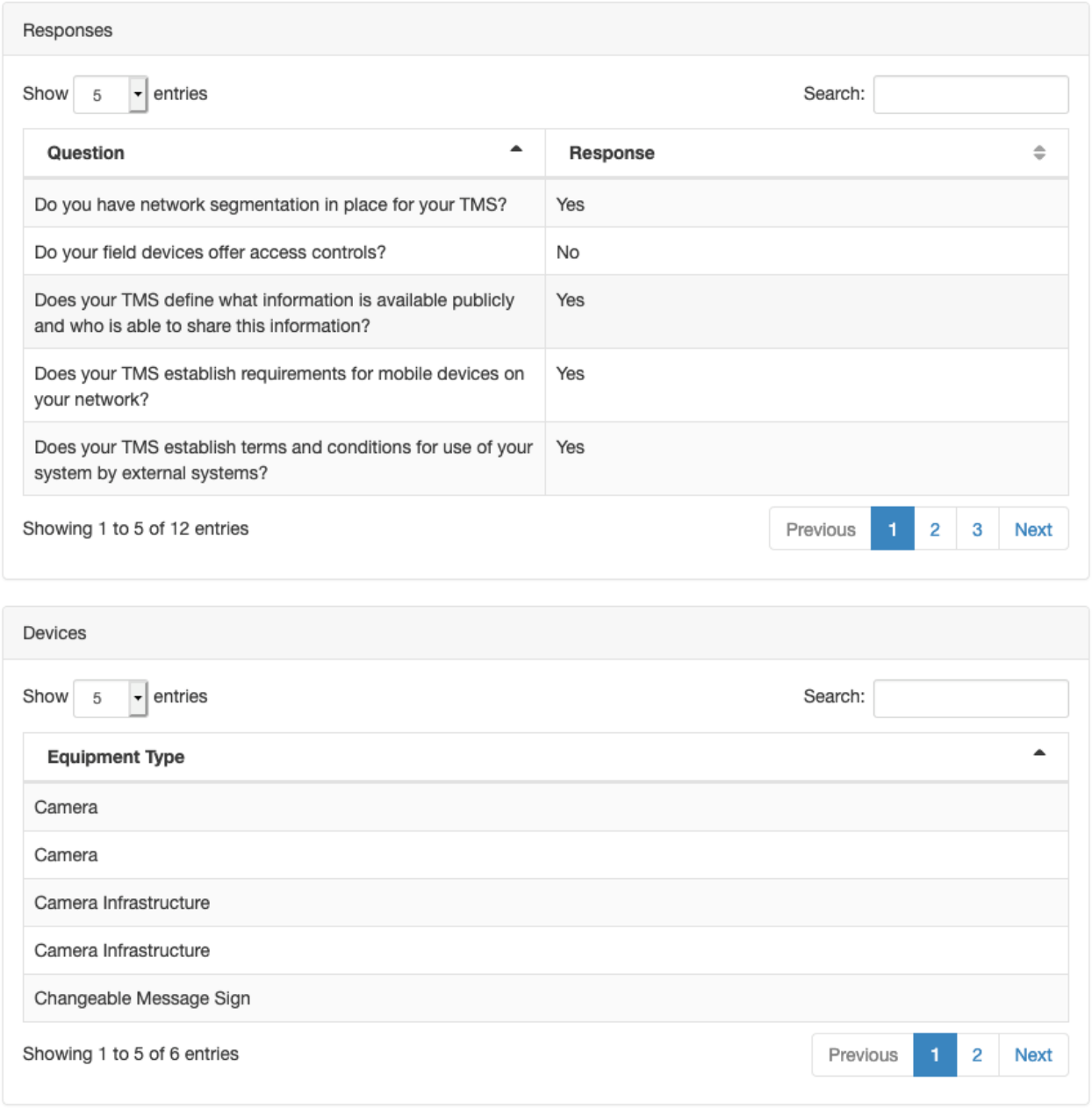

Figure 10. WGT - Cyber Guidance Results Summary Report – Part 2

3.1.2.1.1 Results Download

The first portion of the "Results" page, shown in Figure 11, presents the user a link to download their Cyber Guidance Report in the form of an encrypted Client Information File (CIF), which can be reuploaded in the landing page for easy access to their results, as discussed in section 3.1.2.2. When the "Download" button is clicked, the user will have the opportunity to input the filename for their CIF and it will then be saved on the user's PC in the "Downloads" folder.

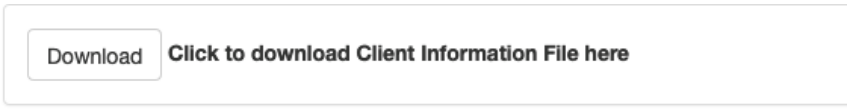

Figure 11. WGT - Cyber Guidance Results Summary – Results Download

3.1.2.1.2 Print Report

Directly below the "Results Download" section is the "Print Report" section, shown in Figure 12. In this section, the user can download a print-friendly version of their report, complete with all graphs and tables seen in the "Results" page.

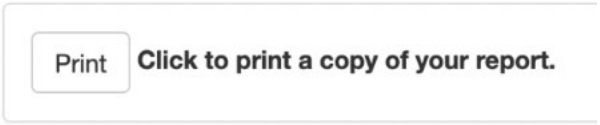

Figure 12. WGT - Cyber Guidance Results Summary - Print Report

3.1.2.1.3 Scoring By Group and Scoring By Question

The "Scoring by Group" displays color-coded graphs corresponding to the user's normalized score by security access control grouping. The "Scoring by Question" displays a radar-chart of the user's score per question. If a group was marked not applicable, it will be excluded from the display. In the example shown in Figure 13, only Access Control and Identification and Authentication were applicable in the user's questioning.

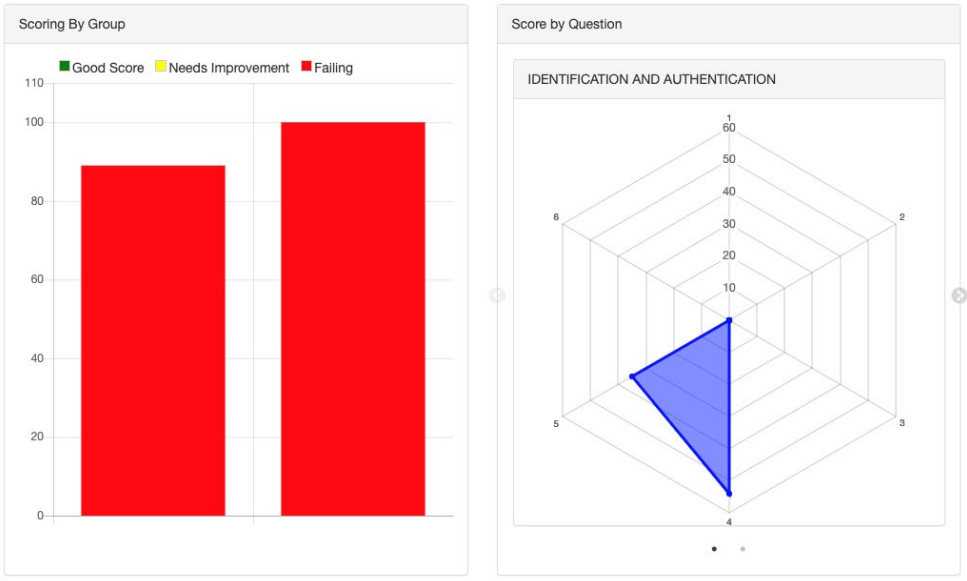

Figure 13. WGT - Cyber Guidance Results Summary - Scoring By Group and Scoring By Question

There are 4 rankings of scoring as follows:

- Negligible –normalized scoring is less than or equal to 0 or 'n/a' (i.e. score =<0 or not applicable)
  - Represented by no bar in the chart "Scoring By Group".
- Low Risk – normalized scoring is greater than 0 or less than or equal to 35 (i.e. 0 < score =<35)

  - Represented by a green bar [ ] in the chart "Scoring By Group".
- Medium Risk – normalized score is greater than 35 or less than or equal to 65 (i.e. 35 < score =<65)
  - Represented by a yellow bar [ ] in the chart "Scoring By Group".
- High Risk – score is greater than 65 or less than or equal to 100(i.e. 65 < score =<100)
  - Represented by a red bar [ ] in the chart "Scoring By Group".

The scoring ranges from 100 to 0, where a score of 0 implies there is a low or negligible cybersecurity risk under this security control versus a score of 100 implies the devices and networks under the TMS have a high cybersecurity risk and additional measures should be taken to reduce these areas of risk as soon as possible.

3.1.2.1.4 Recommendations by Group

Figure 14 presents the recommendations to the risk assessment that are displayed by group and correspond to the risk score in each group.

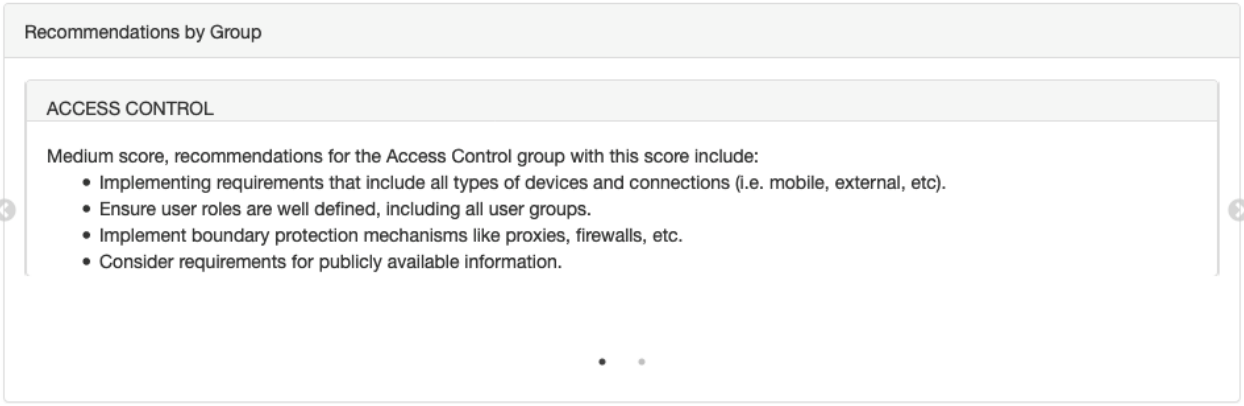

Figure 14. Cyber Guidance Results Summary - Recommendations

3.1.2.1.5 Risk Assessment Response Review

To assist the user with understanding how the scoring took place, the next two sections, shown in Figure 15, present the user's device selections and answers to the security questionnaire.

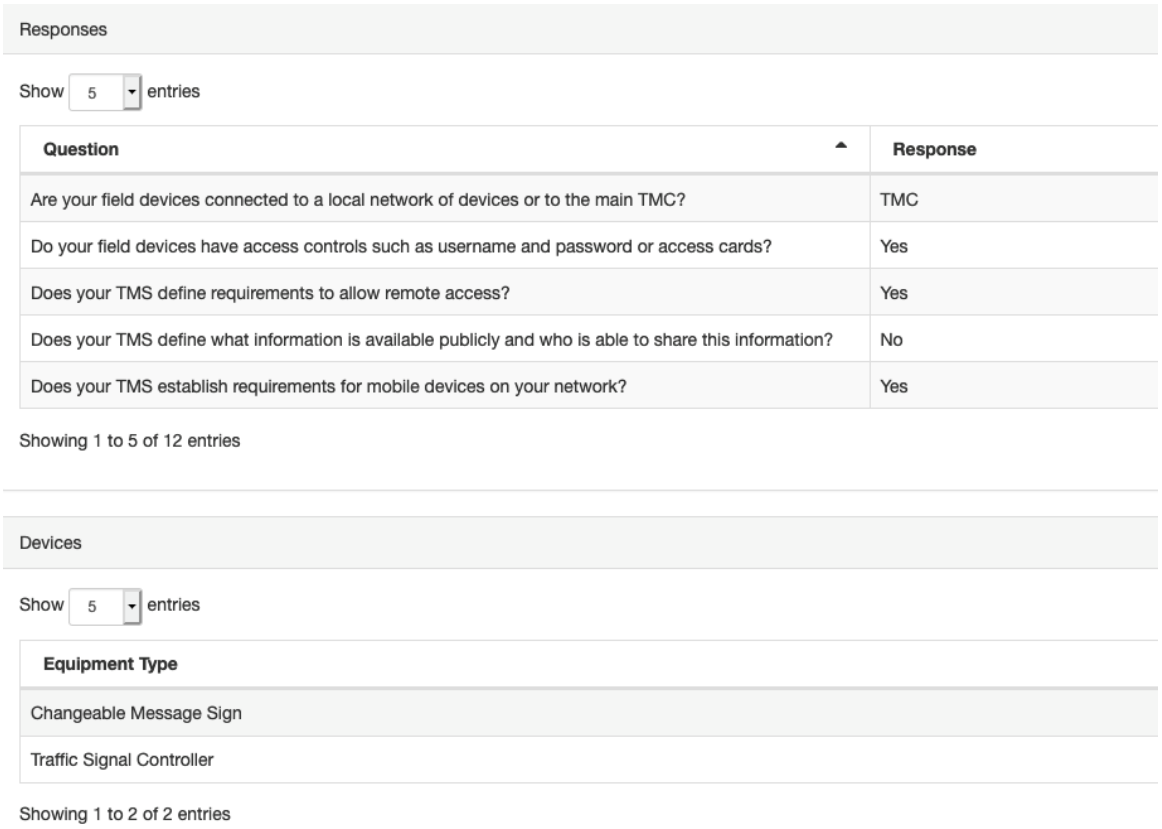

Figure 15. WGT - Cyber Guidance Results Summary – Response Review

3.1.2.2 Viewing of Previous Cyber Guidance Result Summary Reports

The WGT accommodates both offline viewing and previous version comparisons, the results can be saved as an encrypted, timestamped data file.

Previous reports – Previous result files can be reloaded and decrypted by the WGT to review and compare to new results. To complete this process, click the “Browse” button seen in the “Returning User” section of Figure 4, select the CIF you would like to view, and then click the “Submit” button. This will redirect the user to the “Results” page seen in Figure 24.

Offline Viewing – For offline viewing, results will have to be printed to a PDF file and may be stored for offline review.

Cyber Guidance Result files are by default stored under the “Web Guidance Tool” directory and have the following storage format:

[DATE-TIME]_[NAME_OF_REPORT]

These reports can only be opened by the WGT at this time as they are encrypted for end-user data privacy as shown in the Figure 16.

Figure 16. Example Cyber Guidance Report Encrypted

3.2 Troubleshooting

The following sections are intended to assist if an unexpected error occurs.

3.2.1 Resetting User Password

In the case that a user forgets their password, they will need to click the “Forgot Password?” link on the login page. After clicking the link, the user will be asked to enter their email associated with their account, as shown in Figure 17. An email will be sent to this account containing a link that will allow a user to reset their password.

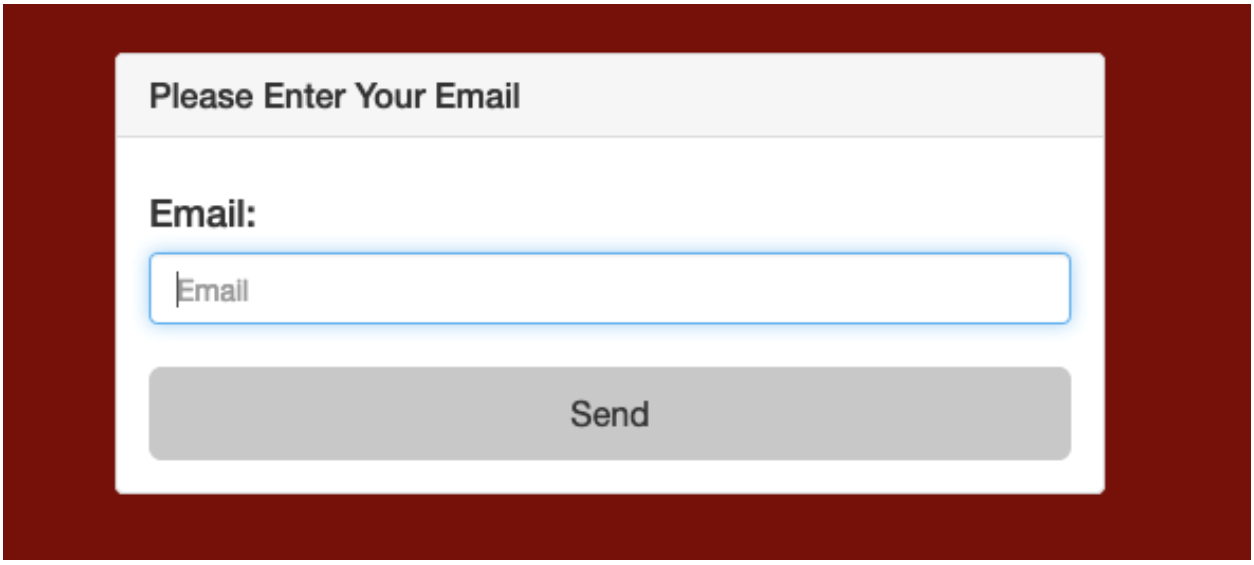

Figure 17. WGT - Password Reset Page

3.3 Messages

The following section will describe the two (2) types of messages the user may encounter while using the WGT web interface, Validation Messages and Confirmation Messages.

3.3.1 Validation Messages

Validation messages will mark when a field is required to proceed but was either not entered or incorrect information was entered, an example of this can be seen in Figure 18.

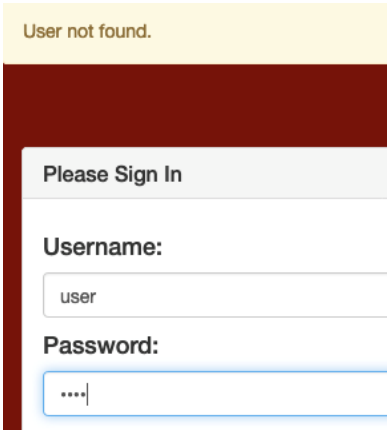

Figure 18. Validation Messages - Incorrect Username

3.3.2 Login Validation Messages

On the Login Page, if no account information is entered and the Login button is pressed, a message stating that the required field(s) are missing and will be displayed as shown in Figure 19.

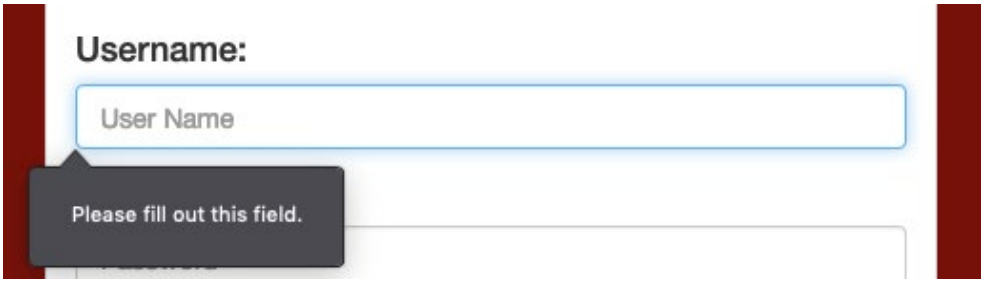

Figure 19. Login Validation Message - Required Fields Missing

If the login account information is invalid, a message above the Login button will be displayed as shown in Figure 20.

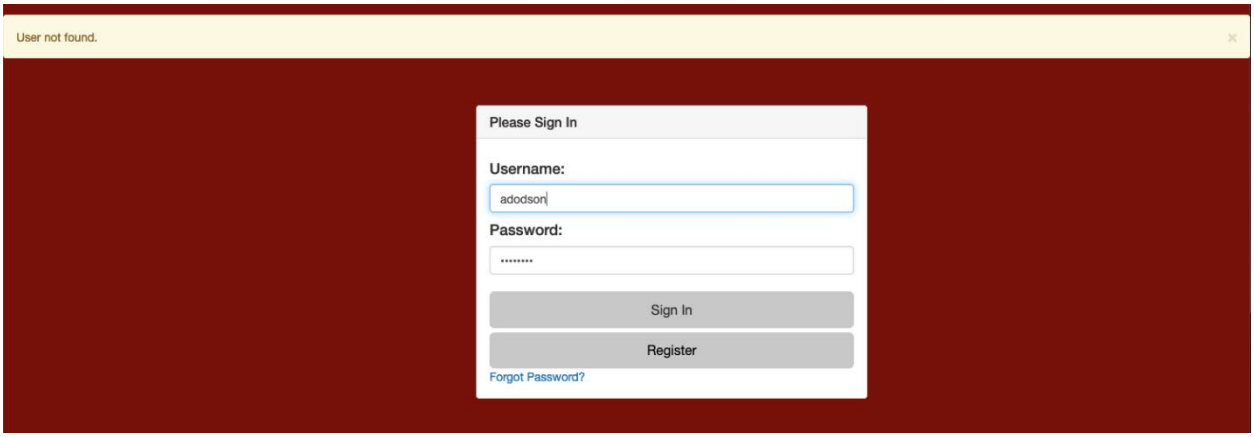

Figure 20. Login Validation Message - Incorrect Login Credentials

3.4 Quick-Reference

The following sections are intended for quick reference on how to accomplish various tasks in the WGT web interface.

3.4.1 Importing Existing Report

The WGT supports importing existing report data through the Upload Report interface. From the main page, click the Returning User section on the lower right corner of the page as shown in Figure 21.

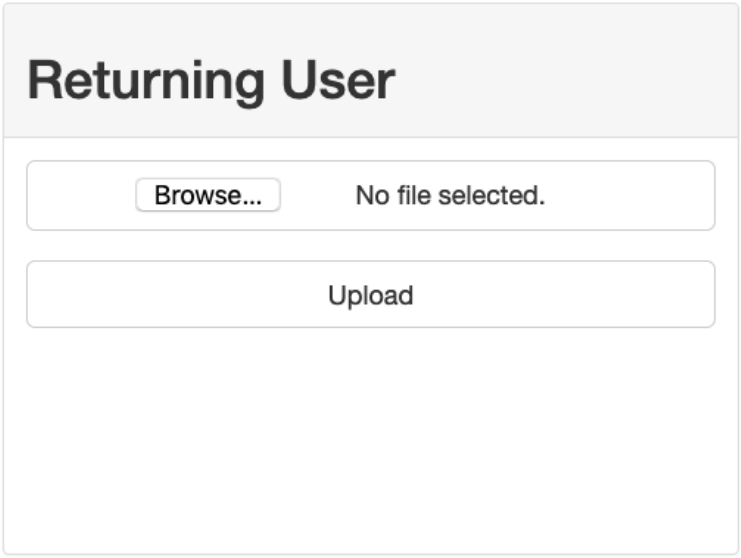

Figure 21. Upload Report Data Link

To upload a previous report, the user will first click the "Browse" link, opening a system file viewer which will open to the last directory the user last saved a file from their web browser, and select the report they wish to view. After selecting the file, the user will click "Upload" to upload the information stored in the report to the WGT. The user will be redirected to the "Results" page to view the report.

3.4.2 Create a New Cyber Guidance Report

To create a new report, the user must complete both the devices and questionnaire portion of the WGT, shown in Figure 22 and Figure 23 respectively. After completing both, the user will select to download the Cyber Guidance Report from the "Results" page, shown in Figure 24. This will prompt a download within the user's web browser, where the user can store a local copy of their results on their local machine for later review.

3.4.2.1 Select Devices

As the WGT does not collect specific device details of each user's TMS, a generic list representation is used. The user will select from Figure 22 the device present in their environment. Many of the high-risk devices present in a TMS are presented in this list of devices.

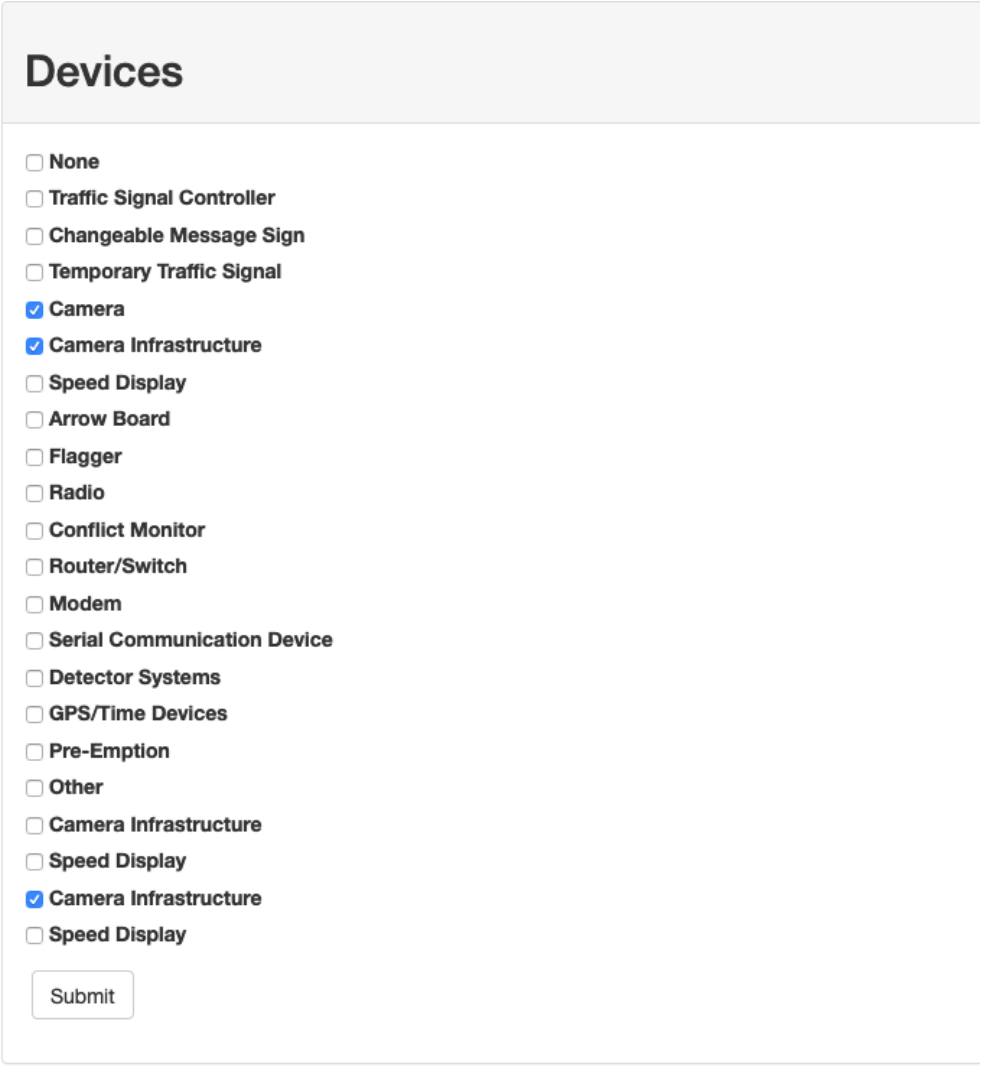

Figure 22. Select Devices Page

3.4.2.2 Answer Questionnaire

When the user selects the “Questionnaire” link, they will be presented with the list of risk assessment questions. Selecting the “i” icon, as shown in Figure 23, will present further information on the question.

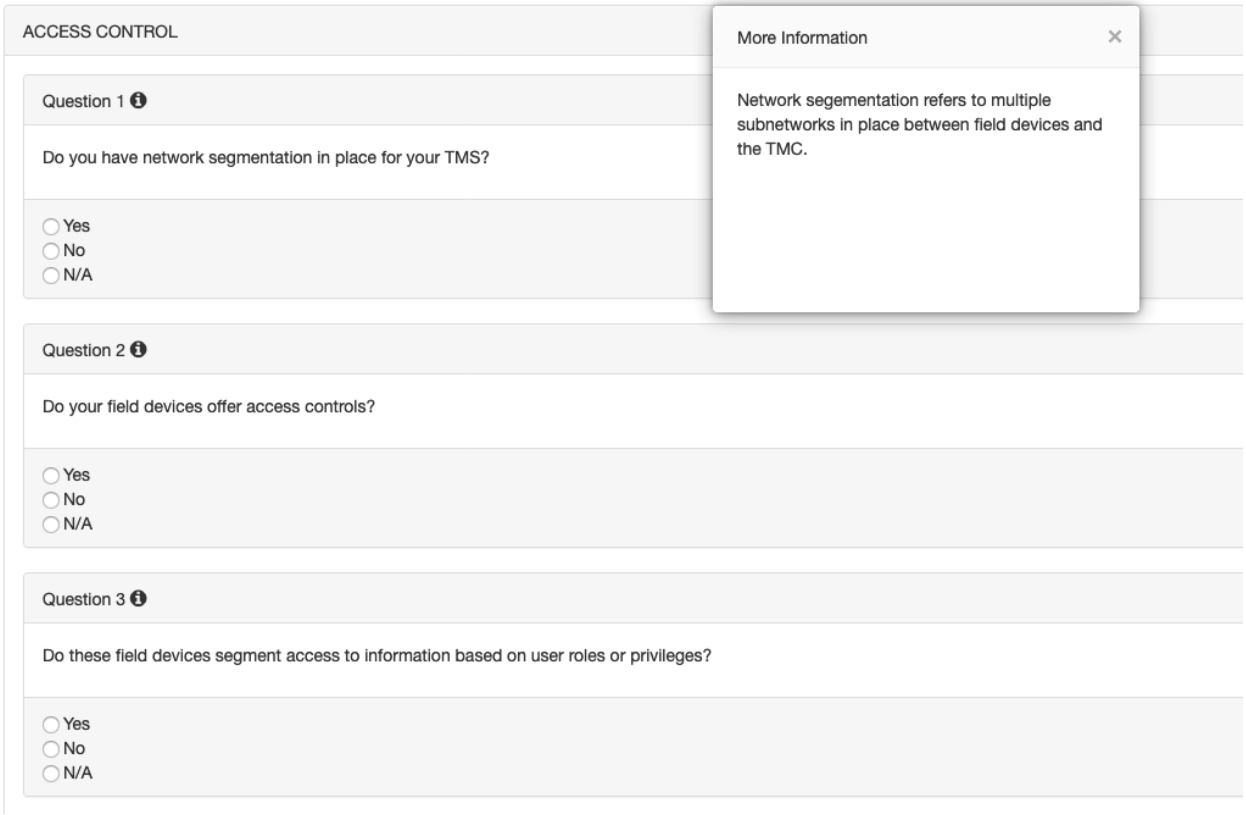

Figure 23. Questionnaire Page

3.4.2.3 View Results

Once both the devices and questionnaire of the risk assessment have been completed, the user can select the results page to view the outcome of their responses, as shown in Figure 24.

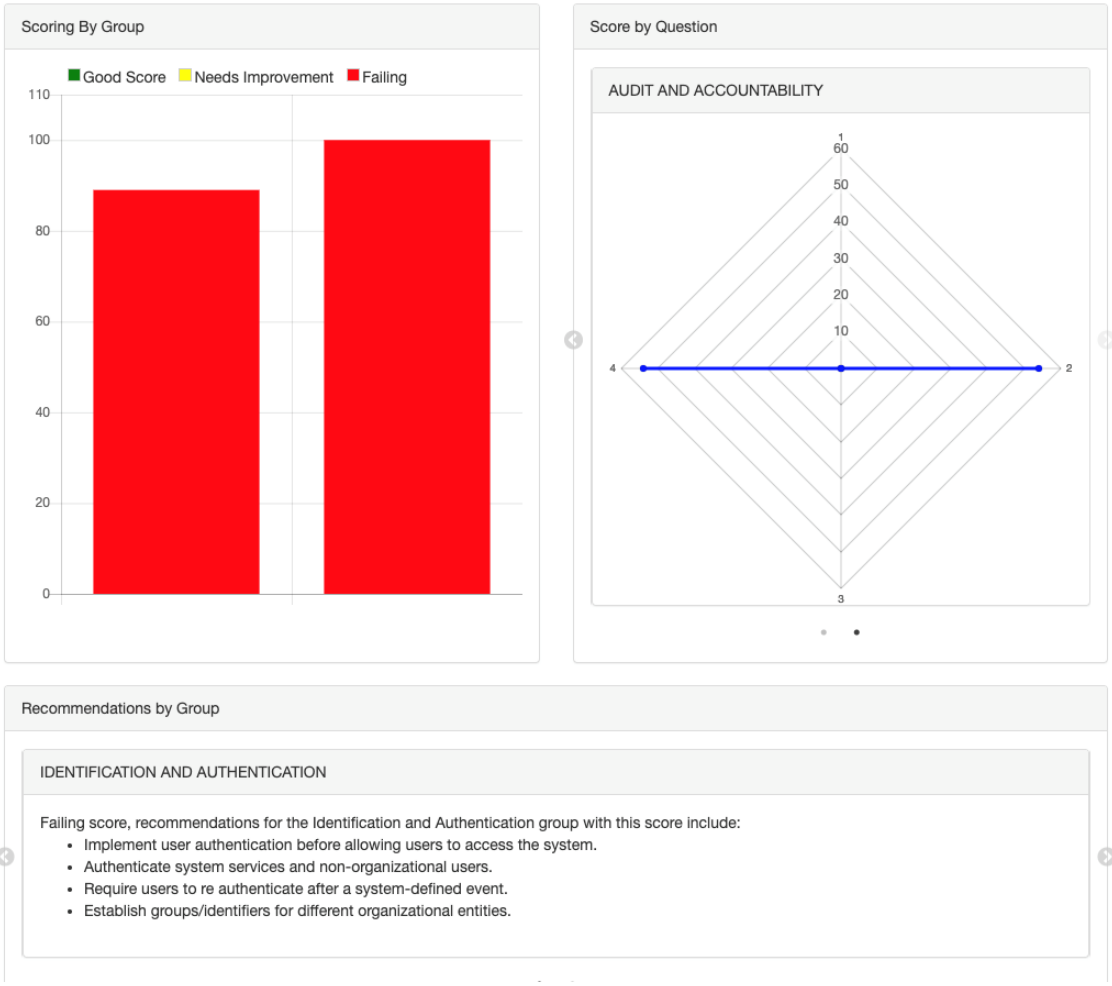

Figure 24. Results Page

APPENDIX A Acronyms

Acronym	Definition
AV	Automated Vehicle
C_2M_2	Cybersecurity Capability Maturity Model
CAV	Connected and Automated Vehicle
CIF	Client Information File
CV	Connected Vehicle
DOT	Department of Transportation
MVC	Model-View-Controller
NOCoE	National Operations Center of Excellence
OS	Operating System
RAM	Random Access Memory
TMS	Traffic Management System
TRB	Transportation Research Board
TSS	Traffic Signal Systems
V2I	Vehicle To Infrastructure
WGT	Web Guidance Tool