Multi Factor Authentication Implementation

Voorhees Township Public Schools

SPELL JIF Virtual Safety Seminar – July 19, 2023

Multi Factor Authentication (MFA)

- MFA protects user data (e.g., personal identification or financial assets) from being accessed by an unauthorized third party, even if the username + password combination is discovered
- MFA is an electronic authentication method - a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors):
    - **Knowledge (something only the user knows)** - Information only known to the user, such as a PIN, etc.
    - **Possession (something only the user has)** - Any physical object in the possession of the user, such as a security token (USB stick), a bank card, a key, etc.
    - **Inherence (something only the user is)** - Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
    - **Location (somewhere the user is)** - Some connection to a specific computing network or using a GPS signal to identify the location
- An unauthorized actor is unlikely to be able to supply all the factors required for access, and is therefore denied access
- A good example of two-factor authentication is the withdrawing of money from an ATM; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out
- Goal is to supplement a user-controlled password with a one-time password (OTP) or code generated or received by an authenticator (e.g. a security token or smartphone) that only the user possesses

Evolving Legislative Requirements

NJ S.B. 3062 (Pending) – proactively align to a recognized cyber framework to uncover and remediate gaps minimizes risks and can provide **"Cybersecurity Safe Harbor"** - defenses that shield organizations from liability when they maintain a cybersecurity program that meet certain prescribed standards

- Cybersecurity program must have administrative, technical and physical components that protect personal or restricted information
- Cybersecurity program must meet one or more of three approaches:
    1. It must reasonably conform to the current version of one or more of the enumerated frameworks for cybersecurity - If the chosen framework is amended, the organization must reasonably conform to the amended guidelines within one year
        - NIST
        - FedRAMP Security Assessment Framework
        - ISO/IEC
        - Center for Internet Security (CIS) Controls
    2. If the personal information covered by the program is regulated by the federal or state government, then the company must comply with the security requirements of FERPA, HIPAA, the Gramm-Leach-Bliley Act, or other applicable federal or state regulations
    3. If the personal information is protected by the Payment Card Industry (PCI) data security standard, then the program must reasonably comply with the current version of the PCI data security standard

Cyber Insurance Requirements (STARR Cyber Liability Policy – SPELL JIF)

Tier 1

(Requires “Yes” Response to All Application Questions)

- Perimeter Firewall in Use
- Antivirus in Use
- MFA For Remote Access
- MFA for Privileged Access
- Backups in Use
- Backups Tested
- Backups Encrypted
- Incident Response Plan in Place
- 3rd Party Vetting in Place

Tier 1: $50,000 Retention & 25% Co-Insurance

Tier 2

(“No” Response to One or More Application Questions)

Tier 2: $100,000 Retention & 50% Co-Insurance

You don’t need to be a cybersecurity expert to mitigate risk . . .

a. Identify your “crown jewels” and research/implement best practices, or adopt an accepted cybersecurity framework, for protecting them

b. Multi-Factor Authentication (MFA), in Voorhees, is a single element in a much more comprehensive strategy based on an accepted framework

c. Voorhees data governance rules and cyber defense strategy is part of the district’s board approved technology plan

d. Goals for MFA:

    a. Encourage staff to voluntarily implement MFA in all data systems they use that support it

    b. Require MFA for Externally-Exposed Applications

    c. Require MFA for Remote Network Access

    d. Require MFA for Administrative Access

Cybersecurity Strategy Based on 3 Elements: People, Process, & Technology

a. People – students, staff and community members having access to data and resources
   - i. Goal: Promote responsible online behavior via end-user assessment, training, and information sharing
   - **ii. Optional MFA** – good cyber hygiene choices; not enforced

b. Process – based on strong data governance policy & procedures
   - i. Goal: ensure confidentiality, integrity, and availability of the district’s data by reducing data security risks due to unauthorized access, handling or misuse of data
   - **ii. Enforced MFA** – policy & procedure based; not optional

c. Technology – multi-layered defense for cloud, email, network, and endpoints via the integration of technology security products
   - i. Goal: prevent and mitigate risk to our exposed data, the devices that provide access, and the users that have that access
   - **ii. Optional or Enforced MFA** – method controlled by the application; optional or mandatory based on data platform

MFA in Broader Context: “VTSD Cyber Defense Gap Analysis & Security Plan”

Based on **Center for Internet Security (CIS)** Best Practices – CIS Controls

- More than a checklist of “good things to do,” or “things that could help”; instead, they are a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements.

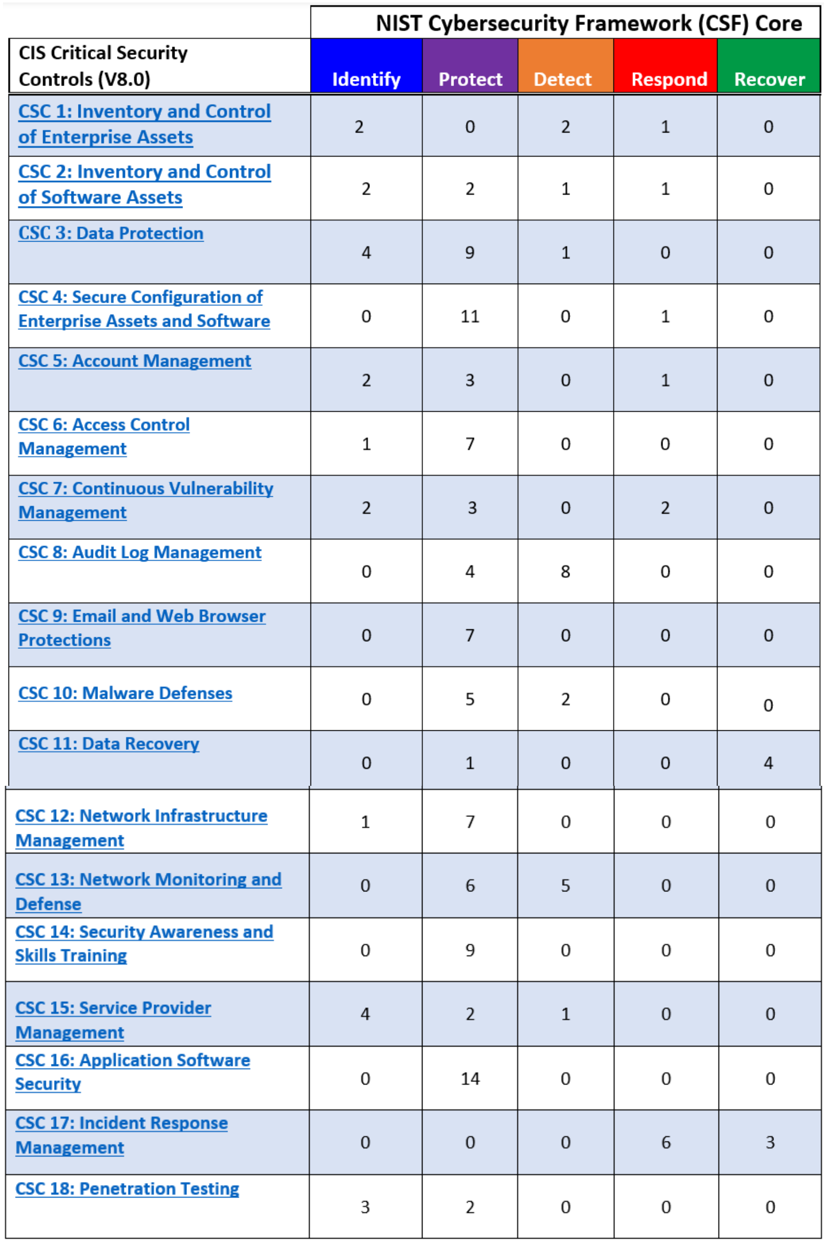
Center for Internet Security®

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security; deliver world-class cyber security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

For additional information, go to <http://www.cisecurity.org/>

18 Critical Security Controls (CSC) – People, Process, Technology

- NIST Cybersecurity Framework (CSF) Category(s) alignment – 5 pillars
- 152 CSC Sub-Control identifiers, each with a thorough description of requirements
- MFA in CSC 6: Access Control Management

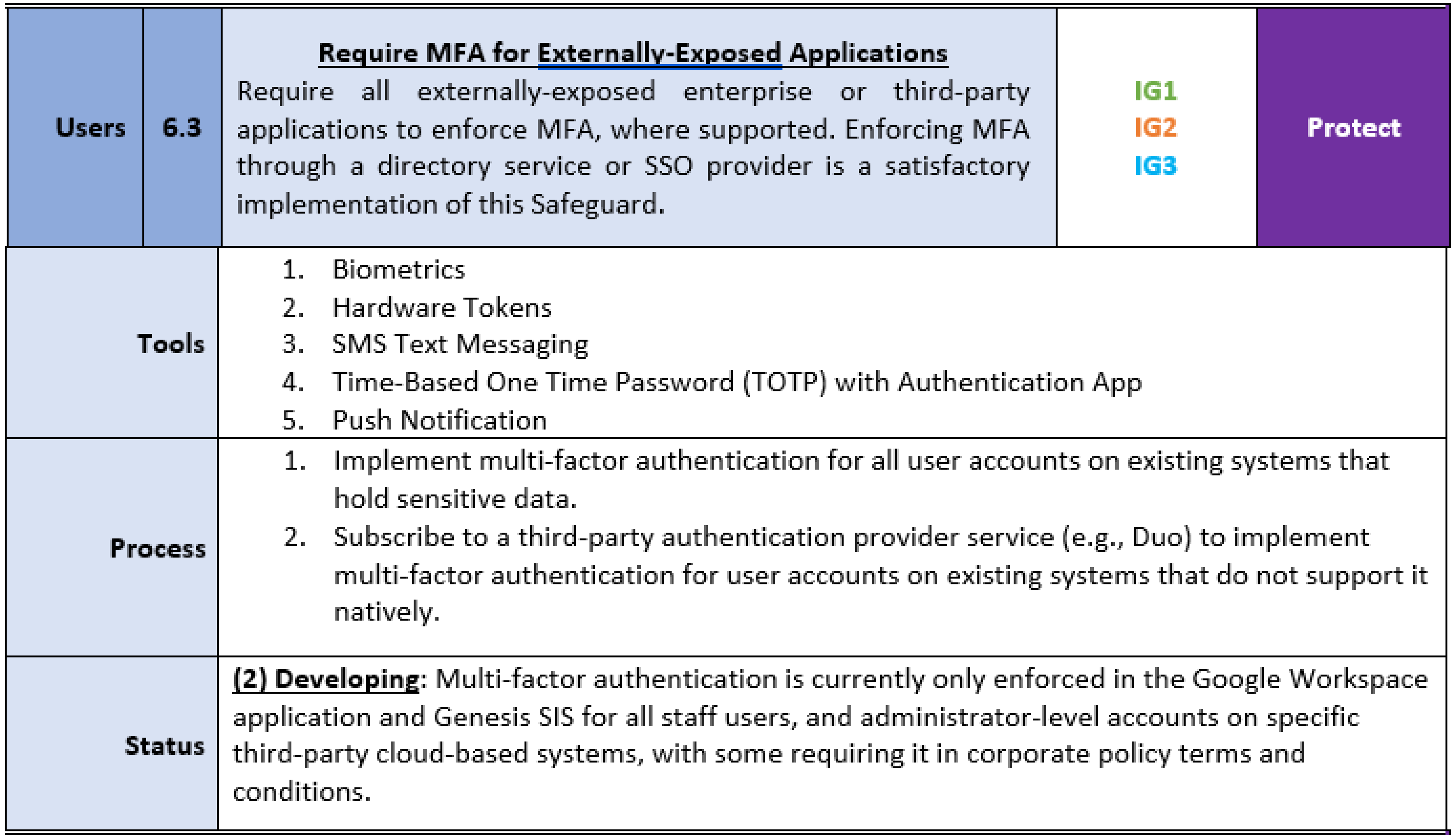


	NIST Cybersecurity Framework (CSF) Core				
CIS Critical Security Controls (V8.0)	Identify	Protect	Detect	Respond	Recover
CSC 1: Inventory and Control of Enterprise Assets	2	0	2	1	0
CSC 2: Inventory and Control of Software Assets	2	2	1	1	0
CSC 3: Data Protection	4	9	1	0	0
CSC 4: Secure Configuration of Enterprise Assets and Software	0	11	0	1	0
CSC 5: Account Management	2	3	0	1	0
CSC 6: Access Control Management	1	7	0	0	0
CSC 7: Continuous Vulnerability Management	2	3	0	2	0
CSC 8: Audit Log Management	0	4	8	0	0
CSC 9: Email and Web Browser Protections	0	7	0	0	0
CSC 10: Malware Defenses	0	5	2	0	0
CSC 11: Data Recovery	0	1	0	0	4
CSC 12: Network Infrastructure Management	1	7	0	0	0
CSC 13: Network Monitoring and Defense	0	6	5	0	0
CSC 14: Security Awareness and Skills Training	0	9	0	0	0
CSC 15: Service Provider Management	4	2	1	0	0
CSC 16: Application Software Security	0	14	0	0	0
CSC 17: Incident Response Management	0	0	0	6	3
CSC 18: Penetration Testing	3	2	0	0	0

NIST Security Functions associated with each CIS Critical Security Control

CSC 6: Access Control Management

- **CSC 6.3 “Require MFA for Externally-Exposed Applications”**
- Target Implementation Group identified
- Tools currently available to the district’s IT department for addressing each Sub-Control
- Process for meeting the required task(s) described
- Status rating and statement based on reflection of process as related to known best practices - Current Rating: 2 out of possible 4 – need to expand beyond Google Workspace & Genesis SIS
- Annual review conducted



Users	**6.3**	**Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. Biometrics 2. Hardware Tokens 3. SMS Text Messaging 4. Time-Based One Time Password (TOTP) with Authentication App 5. Push Notification		
Process		1. Implement multi-factor authentication for all user accounts on existing systems that hold sensitive data. 2. Subscribe to a third-party authentication provider service (e.g., Duo) to implement multi-factor authentication for user accounts on existing systems that do not support it natively.		
Status		**(2) Developing**: Multi-factor authentication is currently only enforced in the Google Workspace application and Genesis SIS for all staff users, and administrator-level accounts on specific third-party cloud-based systems, with some requiring it in corporate policy terms and conditions.		

CIS Critical Security Controls – Voorhees Township School District Gap Analysis

For each of the CSC Sub-Controls there is a “Status” component. The Status section contains both a rating and a description representing the condition of our current efforts as they relate to completion of the stated objective(s). Information is provided here by district IT department staff following internal reflection and evaluative discussions. Although the narrative portion of this component is self-explanatory, the rating scale used here for each Sub-Control is as follows:

- **Aspiring** (**1 Point**) – Task(s) is under consideration, however not currently being pursued as more information, resources or assistance is required.
- **Developing** (**2 Points**) – Task(s) is partially addressed using available tools and processes, however additional effort and resources are needed to see it through completion.
- **Maintaining** (**3 Points**) – Task(s) has been met satisfactorily using current tools and processes, however focus does not expand beyond what has been stated in the document.
- **Enhancing** (**4 Points**) – Task(s) has been met satisfactorily using current tools and processes, and additional efforts have been made to identify and address other related issues.

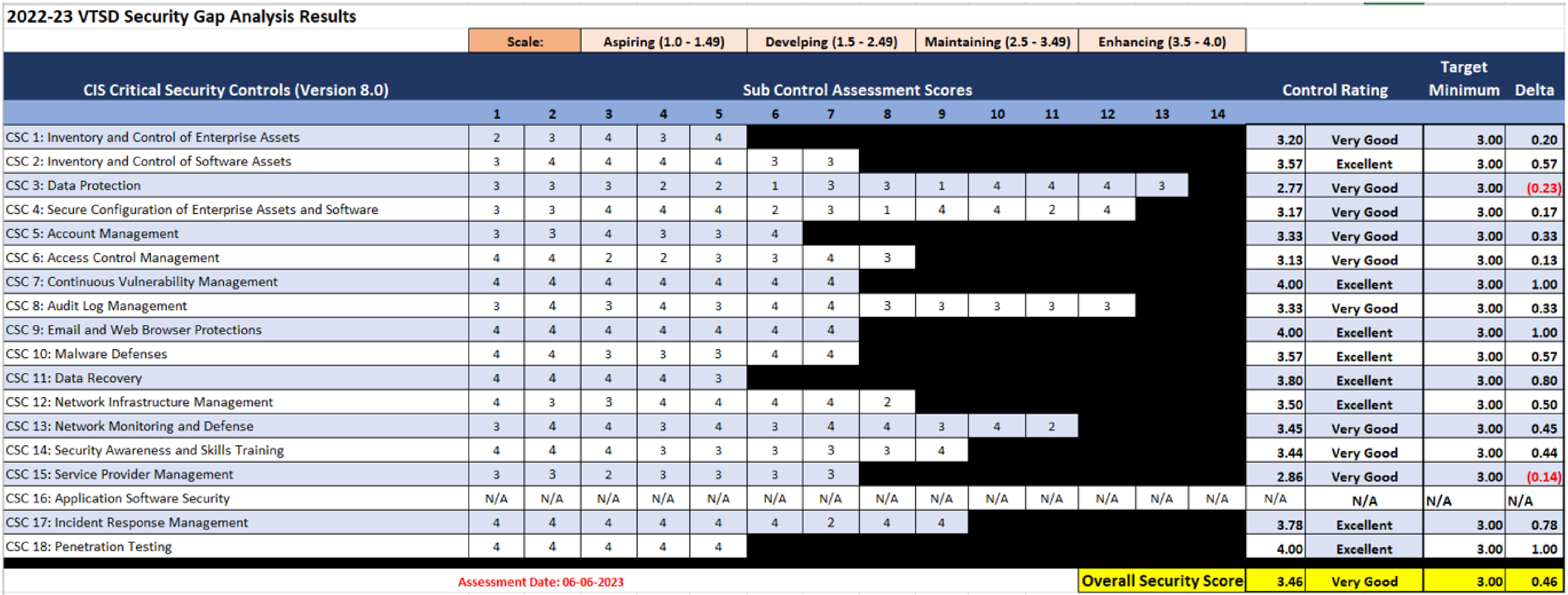
CIS Critical Security Controls – Voorhees Township School District Gap Analysis

The rating assigned to each CSC is calculated by taking an average of the ratings assigned to each of its Sub-Controls. A scoring range has been defined for each CSC for use in determining its consolidated rating:

- **Poor/Fair** (**1.0 -1.49 Points**)
- **Good** (**1.50–2.49 Points**)
- **Very Good** (**2.50–3.49 Points**)
- **Excellent** (**3.50-4.00 Points**)

The **target for minimum acceptance is 3.00** (the median score in the range for "**Very Good**") and the difference represents the gap. Efforts will be made by the district's IT staff going forward to close each gap by pursuing and completing tasks in each of the Sub-Controls. Based on this analysis**,** the district's **Current Overall Critical Security Rating is 3.46 - "Very Good."**

CIS Critical Security Controls – Voorhees Township School District Gap Analysis



2022-23 VTSD Security Gap Analysis Results

Scale:	Aspiring (1.0 - 1.49)	Develping (1.5 - 2.49)	Maintaining (2.5 - 3.49)	Enhancing (3.5 - 4.0)

CIS Critical Security Controls (Version 8.0)	Sub Control Assessment Scores														Control Rating		Target Minimum	Delta
	1	2	3	4	5	6	7	8	9	10	11	12	13	14				
CSC 1: Inventory and Control of Enterprise Assets	2	3	4	3	4										3.20	Very Good	3.00	0.20
CSC 2: Inventory and Control of Software Assets	3	4	4	4	4	3	3								3.57	Excellent	3.00	0.57
CSC 3: Data Protection	3	3	3	2	2	1	3	3	1	4	4	4	3		2.77	Very Good	3.00	(0.23)
CSC 4: Secure Configuration of Enterprise Assets and Software	3	3	4	4	4	2	3	1	4	4	2	4			3.17	Very Good	3.00	0.17
CSC 5: Account Management	3	3	4	3	3	4									3.33	Very Good	3.00	0.33
CSC 6: Access Control Management	4	4	2	2	3	3	4	3							3.13	Very Good	3.00	0.13
CSC 7: Continuous Vulnerability Management	4	4	4	4	4	4	4								4.00	Excellent	3.00	1.00
CSC 8: Audit Log Management	3	4	3	4	3	4	4	3	3	3	3	3			3.33	Very Good	3.00	0.33
CSC 9: Email and Web Browser Protections	4	4	4	4	4	4	4								4.00	Excellent	3.00	1.00
CSC 10: Malware Defenses	4	4	3	3	3	4	4								3.57	Excellent	3.00	0.57
CSC 11: Data Recovery	4	4	4	4	3										3.80	Excellent	3.00	0.80
CSC 12: Network Infrastructure Management	4	3	3	4	4	4	4	2							3.50	Excellent	3.00	0.50
CSC 13: Network Monitoring and Defense	3	4	4	3	4	3	4	4	3	4	2				3.45	Very Good	3.00	0.45
CSC 14: Security Awareness and Skills Training	4	4	4	3	3	3	3	3	4						3.44	Very Good	3.00	0.44
CSC 15: Service Provider Management	3	3	2	3	3	3	3								2.86	Very Good	3.00	(0.14)
CSC 16: Application Software Security	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CSC 17: Incident Response Management	4	4	4	4	4	4	2	4	4						3.78	Excellent	3.00	0.78
CSC 18: Penetration Testing	4	4	4	4	4										4.00	Excellent	3.00	1.00
	Assessment Date: 06-06-2023											Overall Security Score			3.46	Very Good	3.00	0.46

1st Enforced MFA Implementation:
Google Workspace

Timeline:

1. Following Google Workspace Launch in **2019-20**
   a. There was quite a bit of interest among users to store documents containing sensitive information into Google Drive for sharing and collaboration, as opposed to on our local server storage, but not allowed to do so
   b. Cisco Cloudlock, allows us to parse all documents stored in Google and Office 365 looking for files containing PII, FERPA, IEP, Social Security and other sensitive information for monitoring purposes – violators called out
   c. MFA, as a requirement, became a bargaining chip for allowing staff to store all types of data in Google Drive
2. **Fall, 2020**
   a. Administration announced to staff that we would be changing our user policy in Google Workspace to enforce MFA as part of our cyber security risk mitigation program – a mandate
3. **December, 2020 – February, 2021**
   a. Established the end of February as a deadline to enable MFA voluntarily on Google accounts before enforcement

1st Enforced MFA Implementation:
Google Workspace

Timeline (Continued):

4. During the (**Dec-Feb**) transition period we:
    a. Educated the staff as to the risks for account compromise, as well as the consequences related to data breach - most people understood the message and bought in without much issue
    b. Pushed out and installed the Google Authenticator app on each district-issued staff iPad via our MDM to circumvent any potential concerns about teachers not wanting to use their own personal phone or other device
5. **February 28, 2021**
    a. Changed the user account policy in Google Workspace to enforce MFA in our staff Organizational Units (where staff accounts reside in Google).
6. **March, 2021 and After**
    a. Recommended that staff put Google Authenticator app on their phones too and showed them the other options for satisfying the MFA requirement, e.g., SMS notification, Push notification, etc.

1st Enforced MFA Implementation:

Google Workspace

Relevant Issues:

A. We had some concerns that staff would balk at having to use their personal phone to access the authentication code in Google Authenticator, but since all staff members have a district-issued iPad, for the most part that wouldn't be necessary (although encouraged)

B. We were prepared to implement printable backup codes or purchase security keys (hardware tokens) if needed, but those options never became an issue

C. The ability for staff to "trust" the computer(s) or other device(s) they use regularly made the process relatively painless as well, as it reduced the frequency of having to obtain that second factor during sign in on a designated device(s)

D. Another reason for implementing Google Authenticator over some other method is that Genesis, our student information system, only supports the Time-Based One Time Password (TOTP) method for MFA - so now that we’re requiring all staff to have MFA set up on that platform too, Google Authenticator setup and use was already familiar to them

Educational Technology Consortium of South Jersey (ETCSJ) Discussion Thread #1

Question: Does anyone use Google 2-Factor Authentication? If so, has anyone had to deal with staff members who refuse to use their personal cell phone to activate 2-Factor?

- **Logan Township:** We do use Google 2-Factor, and we did run into the same issue with some staff members. Their argument was they weren't being paid to use their personal devices for work purposes. We met with the union president and explained we let the teachers use their phones on the guest network and expected no compensation in return, and we would appreciate the same courtesy since we could take the position that we're not allowing personal devices to use district resources. The union president completely understood that, and we soon had full buy-in.
- **Berlin Township**: We also allow the teachers to use our guest network for their phones. This gives me a good counter argument.
- **Westampton Schools:** There are codes that can be printed out if they don't want to use their phones.

Educational Technology Consortium of South Jersey (ETCSJ) Discussion Thread #1 (Continued)

Question: Does anyone use Google 2-Factor Authentication? If so, has anyone had to deal with staff members who refuse to use their personal cell phone to activate 2-Factor?

- **Northern Burlington County Regional:** We presented MFA as a way to protect not only student information but, more importantly, the staff's personal information. We also made the argument that this is a common practice with many financial institutions, college tuition portals, and even utility companies that we use daily. These institutions require us to have an MFA. We also created a separate, secure staff WIFI for the staff because some staff were not comfortable putting their personal devices on the guest WIFI. It has been just over a year since we implemented MFA, and we would hear complaints every so often, but overall, we really do not hear anything anymore. It can be tough in the beginning.
- **Mount Ephraim**: I guess I have been lucky as I haven't had any complaints about using MFA. I always put the fear of God in them about cybersecurity so whenever I introduce something new, they all understand why.
- **Pittsgrove:** For staff that did not want to use their cell phone we made an accommodation available. Make an appointment with IT - we establish MFA via a District cell phone and then give them 10 codes to use. NO ONE took this path, the reality that they would have to make time and jump through some hoops worked as a deterrent. We got 100% buy-in via the normal process.

Educational Technology Consortium of South Jersey (ETCSJ) Discussion Thread #2

Question: For those of you that provide a hardware token / security key (YubiKey) to your staff, can you share what model YubiKey you use?

- **Millville:** We use DUO with the YubiKey 5 NFC
- **Mantua Township:** We ordered the 4 Nano just for the tech team. They work well.
- **Delran**: So, I went with the Feitian K9 USB security key instead since they were cheaper. I am glad I went the cheaper route since a lot of people who chose the security key decided they didn’t want them once they received them.

2nd Enforced MFA Implementation:
Genesis Student Information System

Timeline:

1. **2008-09**
   a. MFA option has been available since we started using the product - now that we have everyone doing this in Google Workspace, we decided 2021-22 would be a good time to move forward here as well.
2. **2021-22**
   a. Used new Cyber Insurance policy requirements for managing rising premiums and deductibles as one of our arguments for further hardening our data systems.
3. **Fall, 2021**
   a. Administration announced to staff that we would be changing our user policy in Genesis to enforce MFA as part of our cyber security risk mitigation program – a mandate

2nd Enforced MFA Implementation:
Genesis Student Information System

Timeline (Continued):

4. **November 2021 – January, 2022**
    a. Voluntary user MFA transition period
    b. Reinforced the risks for account compromise with staff, as well as the consequences related to data breach - most people understood the message and bought in without much issue
5. **January 31, 2022**
    a. All user accounts required to have MFA enabled
    b. User account status verified via Genesis Reporting, as global enforcement option not available

2nd Enforced MFA Implementation:
Genesis Student Information System

Relevant Issues:

A. Enabling MFA in Genesis was a user-by-user manual process, so our building technology staff gathered small groups of departments, grade level or content area staff, transitioning these groups in chunks over time

B. Some pushback was expected with this scenario as there is no “trust this computer” option in this environment, so using Google Authenticator will be a requirement for all at every sign in – complaints have been minimal

C. Continued reinforcement of the importance of MFA in risk management as a reason for policy change (mandate), and with the new cyber insurance compliance focus, that has helped us to sell the process

Future MFA Implementation Plans

Other Data Platforms:

1. **Apple and Microsoft** - MFA is currently optional and recommended for anyone using available storage, but we've instructed staff not to store sensitive data in those spaces
    a. MFA is enforceable if eventually deemed to be necessary – optional for now
2. **Systems 3000** - Our accounting and personnel package requires VPN access, so MFA is not a requirement for users
    a. Site-to-site VPN tunnel is set up between our internal network and the hosting site
    b. Remote users must use a private VPN connection
3. **Frontline Special Ed** (Formerly IEP Direct)
    a. Currently, Frontline does not provide MFA - It’s on the road map but not yet available
    b. Moving to implement a 3rd party provider (e.g., Cisco Duo) this summer

Future MFA Implementation Plans (Continued)

4. **Single Sign-On Providers**
   a. Login with **Google** (Microsoft or Apple)
   b. **eDirectory** - Our local server storage environment may be accessed via a storage access portal, **Filr**, for staff remote access
      i. Although this portal encrypts data during transit, and we have implemented complex password and periodic change requirements by policy, this environment does not support MFA natively - Planning a 3rd party MFA solution, **Cisco Duo**, for implementing MFA over LDAP (our internal directory)
      ii. MFA will, as a result, extend to other external systems currently using LDAP authentication: **VPN** Remote Access, **Blackboard** Web Community Manager (district website), **Follett Destiny** Library Management, **Safari Montage**, **Jamf Pro** MDM, etc.

Future MFA Implementation Plans (Continued)

c. **Clever SSO**

1. MFA available through 3rd party application, Authy, or via SMS text messaging
2. Question as to whether integrated Clever apps and data contain sensitive information worth spending the additional funds to protect (are they crown jewels?)
3. User "Badges" (QR codes containing credentials that may be scanned on a device)

5. **Remote Network Access**

a. Our local network environment may be accessed by users remotely via VPN

b. LDAP Authentication is used for VPN access, and MFA will soon be implemented via Cisco Duo

c. Center for Internet Security (CIS) - **CSC 6.4 "Require MFA for Remote Network Access"**

6. **Network Resource Management**

a. MFA is also a requirement for admin accounts on all our other network management applications

b. Center for Internet Security (CIS) - **CSC 6.5 "Require MFA for Administrative Access"**

MFA Implementation Cautions

MFA Bypass Prevention:

1. Choose authentication apps, hardware tokens, or biometrics over SMS text codes or pop-up push notifications
   a. Cyber threat actors can circumvent SMS text-based codes via **SIM Swapping** (the act of switching a user’s phone number to a separate SIM card controlled by a threat actor)
   b. Advanced Persistent Threat (APT) groups deploying a new tactic, **Prompt Bombing** (annoyance caused be receiving an absurd number of pop-up notifications) can lead to frustration and distraction, and that could cause someone to click away notifications that would allow attackers to access our accounts or to execute malicious code
2. Phishing emails attempt to deliver malware capable of harvesting “session cookies” (server-specific token – allows the browser to re-identify itself to the single unique server to which the user previously authenticated). In a **Pass-the-Cookie Attack**, stolen cookies are injected into a new browser session, allowing threat actors to deceive the browser and appear as an authenticated user.

Summary

a. Voorhees School District has identified its crown jewels and is phasing in MFA based on significance of the resource

b. Consider risk/reward, prioritize what needs protection, establish justification, commit

c. MFA should be implemented within the context of a comprehensive cybersecurity policy/program, not in isolation – there are so many additional risks to consider!

d. Cybersecurity best practices should be set in district goals, and staff must be informed of these to better understand the reason(s) for policy changes/mandates that affect them – communication is key for buy-in

e. Optional vs. enforced MFA decisions must be based on district policy, as an extension of that cybersecurity program and other influential factors

f. The type of MFA tool/method selected largely depends on what is supported by the resource one is trying to protect, if available at all, or an available 3rd party option

g. Understanding alternative options for selected MFA methods may provide a workaround – an alternative to using the personal devices of staff (who may object to doing so), or allow staff to make choices based on personal preference or convenience

h. Any decision on whether to implement a third-party MFA solution, at additional cost, must be made following a value judgement about the worth of the data on the system to be protected

i. Choose more secure MFA methods whenever possible

Questions?