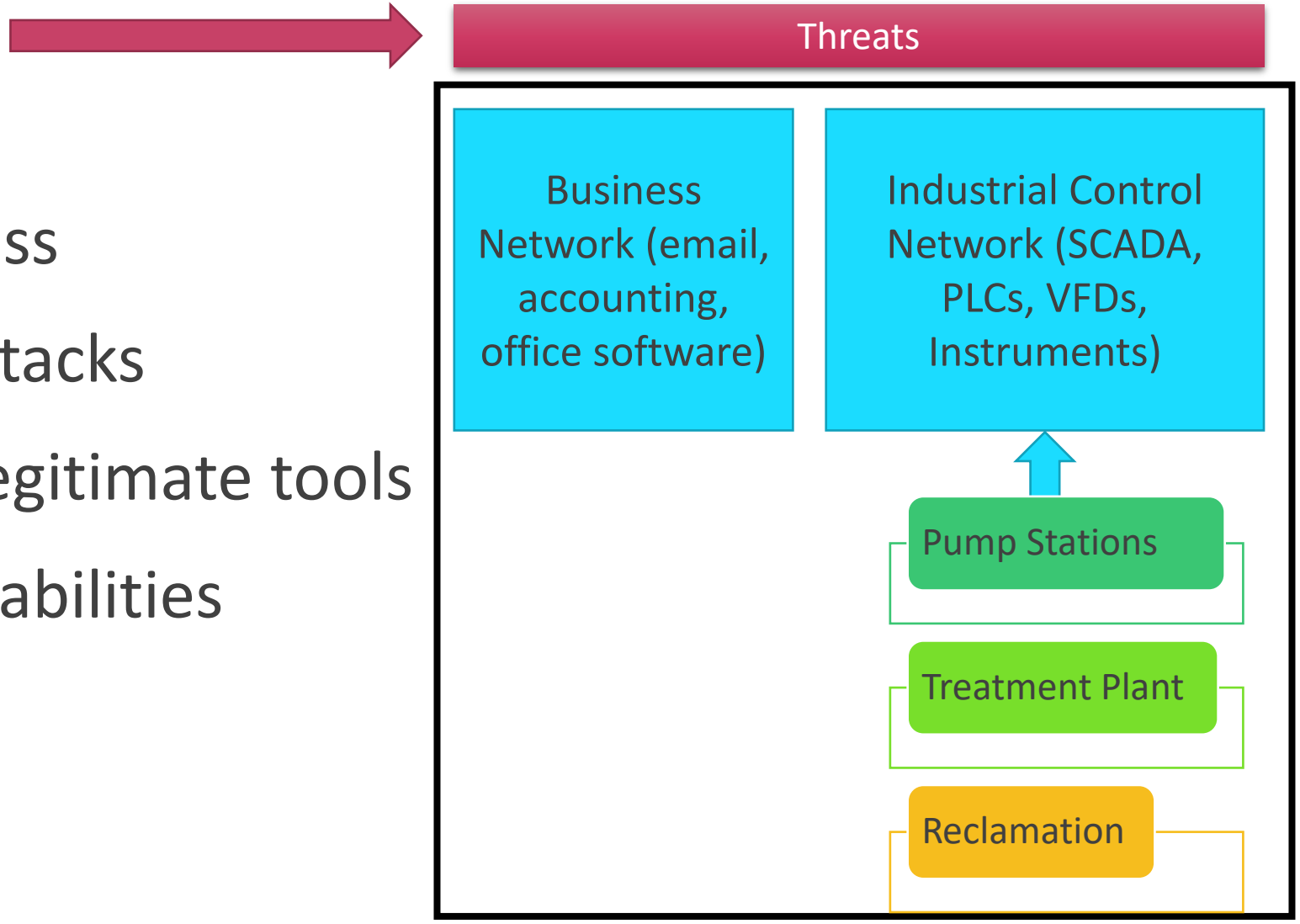
CYBERSECURITY UPDATE

CYBERSECURITY CHALLENGES

- Ransomware
- Secure remote access
- Cloud third party attacks
- Weaponization of legitimate tools
- Supply chain vulnerabilities
- Mobile malware

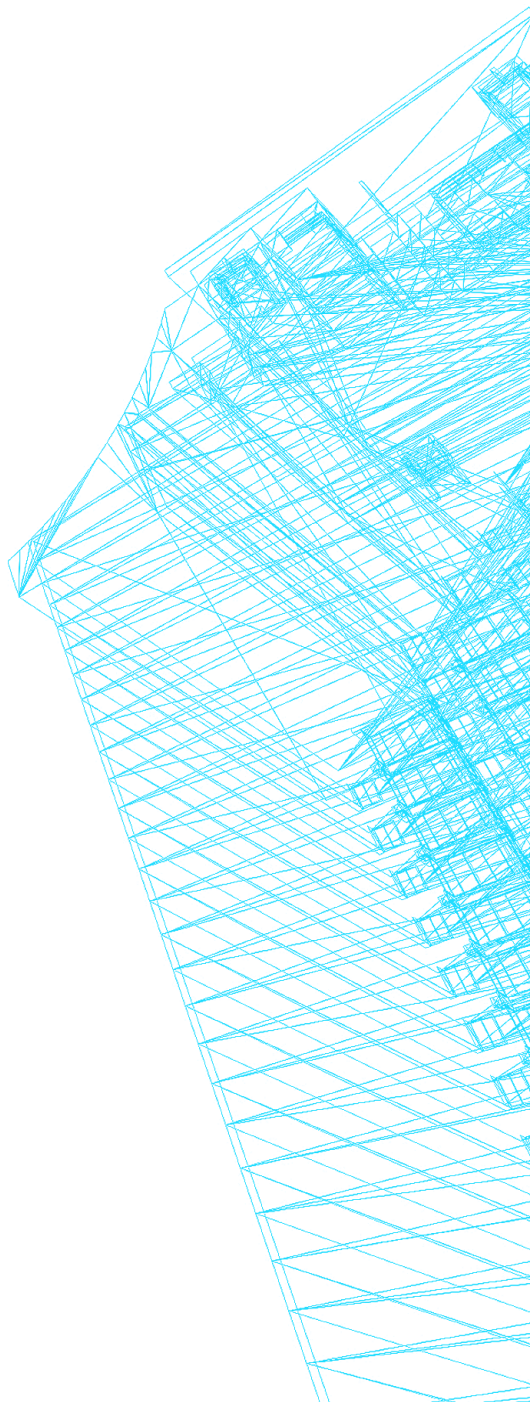


RANSOMWARE

- Annual training for staff and during onboarding of new employees on cybersecurity threats and how to prevent.

- Advanced email filtering implemented with scanning of all links and attachments before email is sent to employee inbox.

- Robust backup system that is validated.



BACKUPS

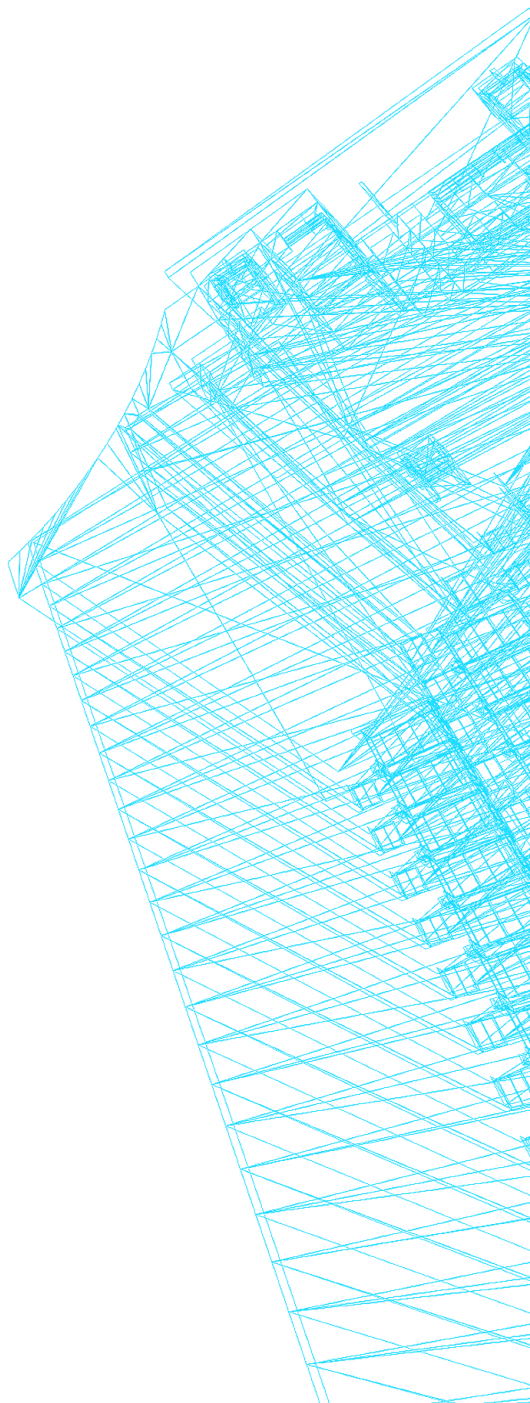
Onsite Backups

Offsite Backups

Offline Backups

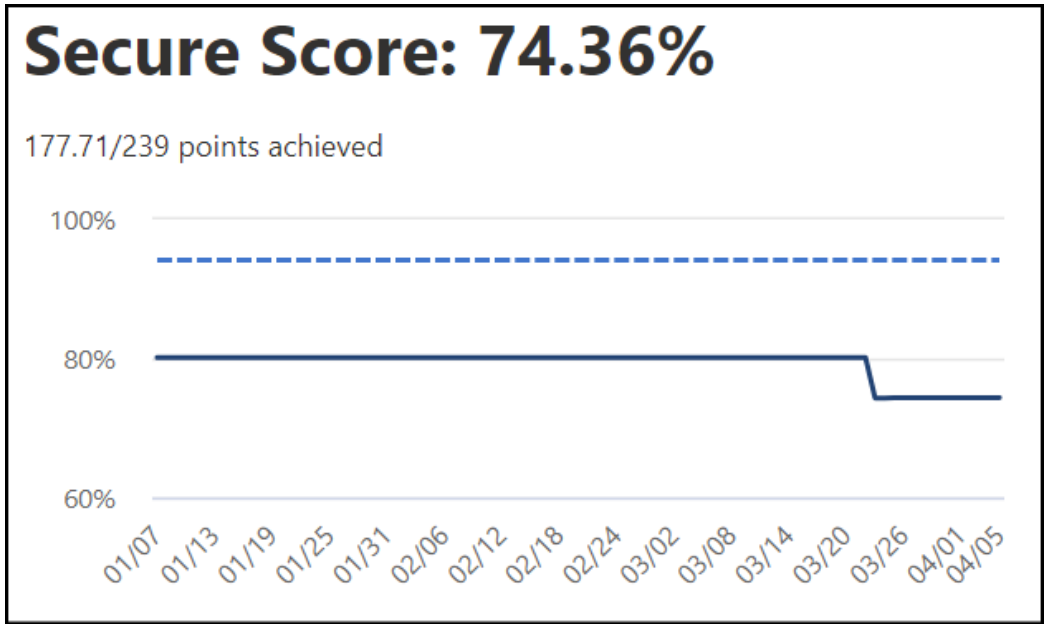
SECURE REMOTE ACCESS

- Audit employee and user access on quarterly basis.
- Remove access immediately when an employee separates from the District.
- Automated expiration of remote access credentials of third-party vendors so they have to request renewal.
- Multifactor authentication for remote access to email and critical infrastructure. SCADA access locked to District devices.



MICROSOFT SECURE SCORE

- Benchmark of security controls that can be compared to similar size businesses.
- Score is currently at 80.16%. It dropped to 74.36% when primary internet was down at the treatment plant.
- Similar size businesses score 47.35%.

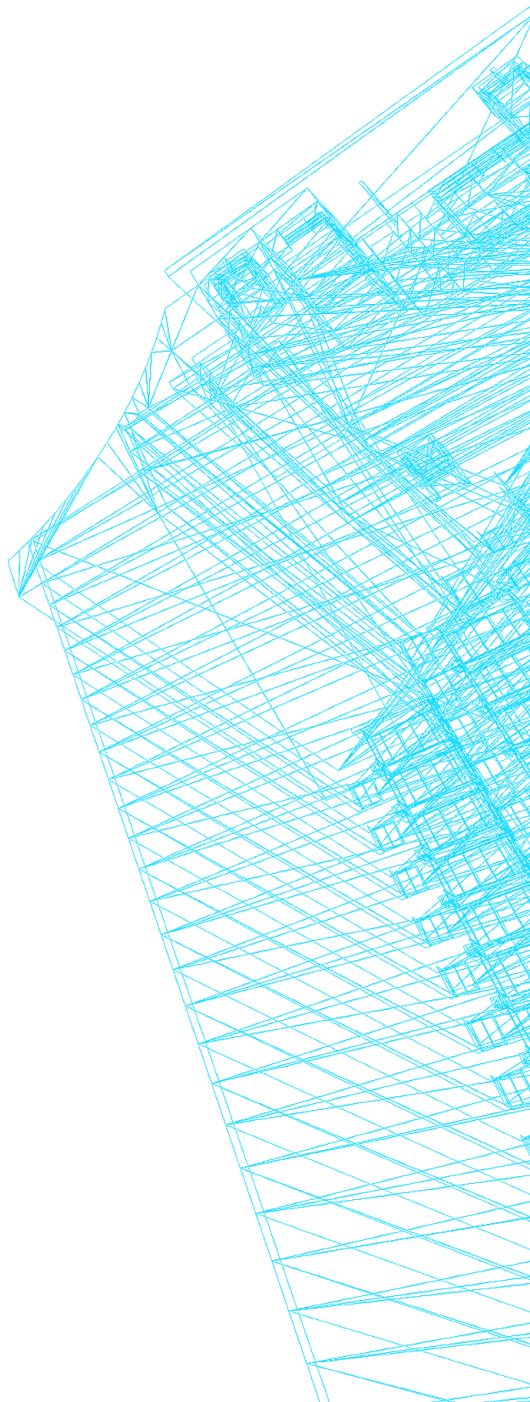


CENTER FOR INTERNET SECURITY-
CRITICAL SECURITY CONTROLS

How this relates to the District

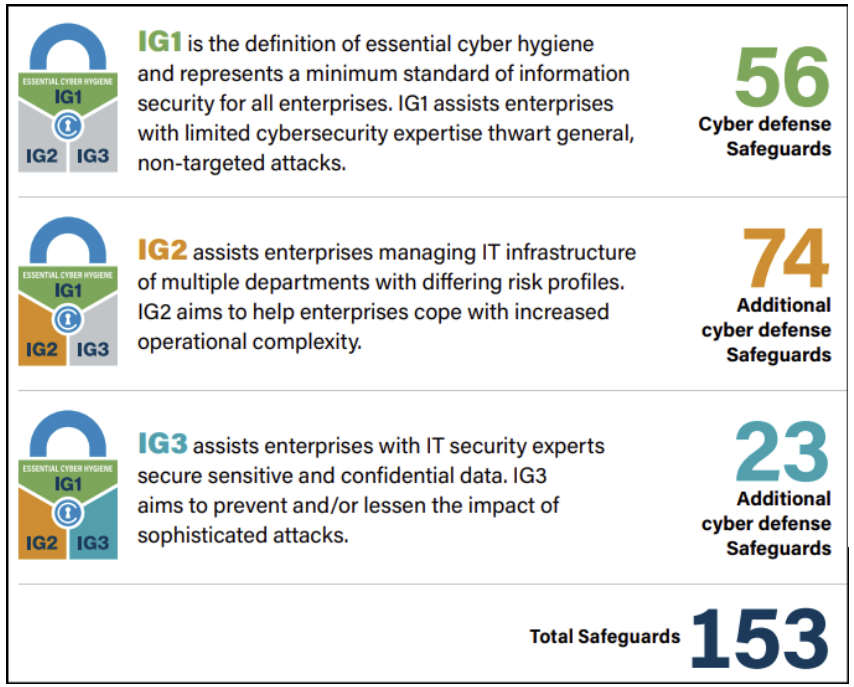
Exceedio has begun an initial assessment to determine the current cybersecurity maturity level of the District based on the controls and safeguards defined by the Center for Internet Security (CIS). For each of the safeguards we are determining:

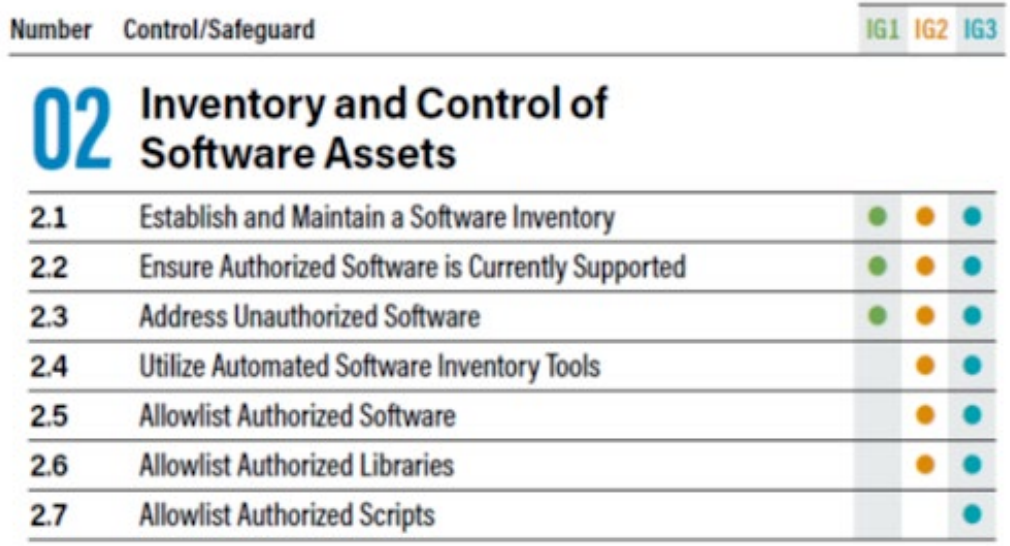
- Is there a policy defined that covers the safeguard?
- To what degree has the safeguard been implemented?
- To what degree has the safeguard been automated or technically enforced?
- To what degree is the District aware of the status of the safeguard?



CENTER FOR INTERNET SECURITY-
CRITICAL SECURITY CONTROLS

Overview of prioritized implementation groups (IG) and example of safeguards.





Number	Control/Safeguard	IG1	IG2	IG3
02	**Inventory and Control of Software Assets**			
2.1	Establish and Maintain a Software Inventory	●	●	●
2.2	Ensure Authorized Software is Currently Supported	●	●	●
2.3	Address Unauthorized Software	●	●	●
2.4	Utilize Automated Software Inventory Tools		●	●
2.5	Allowlist Authorized Software		●	●
2.6	Allowlist Authorized Libraries		●	●
2.7	Allowlist Authorized Scripts			●

NEXT STEPS

Tasks	Target Completion
Contract with new security firm to complete penetration testing.	August 2023
Complete CIS Critical Security Assessment and utilize as action plan to prioritize continued improvements.	June 2023
Automate patch management for industrial control network. It is currently a manual network.	August 2023
Continued training for staff.	Ongoing