COUNTY of VENTURA
Grand Jury

800 South Victoria Avenue
Ventura, CA 93009
Tel (805) 477-1600
Fax (805) 658-4523
grandjury.countyofventura.org

This response was given using the 2020-2021 Ventura County Grand Jury Report form. The form should have reflected the Ventura County Grand Jury Report form 2021-2022.

We regret any confusion this may cause.

Sincerely,

Keith Frost
Foreperson
Ventura County Grand Jury (2022-2023)

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board of Directors
Al E. Fox
Division 1
Jeffrey C. Brown
Division 2
Timothy H. Hoag
Division 3
Eugene F. West
Division 4
Terry L. Foreman
Division 5
General Manager
Tony L. Stafford

Date: July 25, 2022

To: Ventura County Grand Jury

From: Camrosa Water District

Subject: Response to 2020-2021 Ventura County Grand Jury Report – Cybersecurity of Water Providers in Ventura County Findings and Recommendations

The Camrosa Water District agrees with **Finding F-01, The Grand Jury finds that cybersecurity of both IT and SCADA systems is essential to safe and effective delivery of water**. Regarding findings F-02 through F-09, however, the District neither agrees or disagrees with the findings but contends that the Ventura County Grand Jury, Final Report did not provide adequate information to render a decision of the cybersecurity adequacies or inadequacies found among other water agencies within the county.

Regarding the cybersecurity recommendations, the District agrees with **Recommendation R-01, R-03, R-04, R05, and R-06**. The District is in alignment with the recommended cybersecurity controls of the American Water Works Association (AWWA), Water Sector Cybersecurity Risk Management Guidance v3.0, which, in turn, aligns to the National Institute of Standards and Technology (NIST), Cybersecurity Framework v1.1. As part of the AWWA Risk and Resiliency Assessment (RRA), the District, to date, has fully implemented and maintained ninety percent (89 of 99) of the recommended AWWA cybersecurity controls and has partially implemented or is planning seven additional controls. Attached is the District's AWWA RRA Control Output which outlines the District's cybersecurity stature.

Regarding **Recommendation R-02** (recommending public water providers regularly share and exchange information regarding cybersecurity threats, attacks, protections and remedies, and provide training), the District is alignment with AWWAG430.4.3 and DHSCAT-2.11.3 recommendation providing monthly training on a variety of cybersecurity topics including phishing, social engineering, and cyber-hygiene. The District, however, does not regularly share and exchange information regarding cybersecurity threats on any public forum. Any decision to implement such an action would need further analysis and consideration at the Board level.

Sincerely,

Tony Stafford

Tony Stafford
General Manager
Camrosa Water District
805.469.6414

COUNTY *of* VENTURA

Grand Jury

800 South Victoria Avenue
Ventura, CA 93009
Tel (805) 477-1600
Fax (805) 658-4523
grandjury.countyofventura.org

Response to 2020-2021 Ventura County Grand Jury Report Form
(Please See California Penal Code Section 933.05)

Report Title: *Cybersecurity of Water Providers in Ventura County*

Responding Entity: *Camrosa Water District*

FINDINGS

- I (we) agree with the Findings numbered: F-01

- I (we) disagree wholly or partially with the Findings numbered: ____________
  (Attach a statement specifying any portions of the Findings that are disputed; include an explanation of the reasons.)

RECOMMENDATIONS

- Recommendations numbered R-01,R-03,R-04,R-05,R-06 have been implemented.
  (Attach a summary describing the implemented actions.)

- Recommendations numbered ____________ have not yet been implemented but will be implemented in the future.
  (Attach a summary indicating the timeframe for implementation.)

- Recommendations numbered R-02 require further analysis.
  (Attach an explanation to include: scope and parameters of the analysis or study and timeframe for the matter to be prepared for discussion with the agency or department head. The timeframe shall not exceed six months from the date of publication of the report.)

- Recommendations numbered ____________ will not be implemented because they are not warranted or are not reasonable.
  (Attach an explanation.)

Date: 7-25-22

Signed: Tony Stafford

Title: GENERAL MANAGER

Number of pages attached: 11

Date of Tool Usage:	6/30/2022	
Facility/System/Utility:	Camrosa Water District	

AWWA RRA
CONTROL OUTPUT FORM

The RRA-Control Output tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013. This will support the evaluation of risks to and resilience of the following infrastructures as specified by AWIA §2013:

- •electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
- •the monitoring practices of the system (including network monitoring);
- •the financial infrastructure of the system (meaning accounting and financial enterprise IT systems operated by a utility, such as customer billing and payment systems).

Additional Details/Examples are provided for each control. These are designed to provide "real-world" examples of how a utility may implement a control or observe the control in day-to-day operations. The list of potential examples is quite long for some of the controls. Therefore, please consider this to be a non-exhaustive list of examples.

If all of the recommended controls have a "Fully Implemented and Maintained" status, then your utility is taking a robust approach to a risk management.

Tab Instructions:

The Control Status column is the only column that requires additional user input. It is colored blue for identification purposes. The user must select the implementation status of the control within the utility/system/facility under evaluation. The options for implementation levels include:

1. Not Planned and/or Not Implemented – Risk Accepted – The control is not currently implemented or planned for implementation. The organization accepts risks associated with the control not being implemented.
2. Planned and Not Implemented – The control has not been implemented. However, implementation of the control is planned.
3. Partially Implemented – The control is partially implemented by internal or external resources.
4. Fully Implemented and Maintained – The control is fully implemented and actively maintained by internal or external resources.

IF DATA NOT VISIBLE BELOW, PRESS CTRL-ALT-Function 9 KEYS.

TO ENSURE PROPER FUNCTION OF THIS SHEET AND UPLOAD TO CSET, PLEASE DO NOT ADD EITHER ROWS OR COLUMNS TO THIS SHEET

Control ID	Control description	Additional Details/Examples	Priority	Control Status	Improvement Project	Control References	Notes
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	A SCADA tech believes a machine is infected Based on their training, they remove the machine from the network and report it to IT without powering it off to avoid deleting evidence.	1	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.7.7*	*Network traffic is analyzed and logged at the Firewall level. User auditing is logged on Domain Controller - Active Directory.*
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies.	1	Fully Implemented and Maintained	Application Security	*ISA62443-3-3.6, NIST800-82.6.2.3*	*Independent annual business audits have been conducted for the past 2 year. Quarterly TBRs are also conducted now that include auditing of cybersecurity controls.*
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	The process of implementing policies and procedures is clearly defined and reviewed. Updates to this process are made by a responsible party.	1	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.1, ISOIEC27.27001.AA.A.5*	*Per policy, cyber security controls that define levels of information governance, periodic review of practices are in place. See the Camrosa IT Plan for more information.*
AU-3	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	A utility has a required number of accountable staff that must review or provide input before security policies are put in place. Periodic review that approved security policies are being followed.	1	Fully Implemented and Maintained	Governance and Risk Management	*ISA62443-2-1.A.3.2.3, ISOIEC27.27005.WD, NIST800-53.J.AR-1*	*Per policy, cyber security controls are in place that ensure security policies undergo periodic review and ensure these policies are being followed.*
AU-4	Information security responsibilities defined and assigned.	All staff are aware of who they would report to if they notice suspicious behavior in the system.	1	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.6.1.1, NIST800-53.F-AU.AU-1*	*Per policy, the roles and associated duties of each member of the IT Department are clearly defined along with their levels of network access.*
DS-2	A Privacy Policy as well as a Cyber Security Breach Policy are implemented.	An operator knows how to identify and respond to a suspected cyber breach, based on his cybersecurity training.	1	Fully Implemented and Maintained	Data Security	*PII-State Specific*	*Incident reporting procedures are in place. Staff is trained monthly on pertinent cyber security topics*

DS-3	A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.	Current practices are reviewed by legal counsel for legal compliance with HIPAA.	1	Not Planned and/or Not Implemented - Risk Accepted	Data Security	*45 CFR Part 160, 45 CFR Part 164*	*not applicable*
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Based on their knowledge of access control policies, operators do not share passwords.	1	Fully Implemented and Maintained	Access Control	*AWWAG430.4.6, NIST800-82.6.2.1*	*Individual user accounts and passwords with appropriate access levels are maintained. Privilege/system accounts are provided as needed.*
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	If no user is logged in at a SCADA screen, a read-only view is presented. Individual roles created and assigned to users depending on their responsibilities.	1	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.15.11*	*Per policy, information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account.*
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high risk locations.	Access to control of critical equipment is only available at a secured terminal.	1	Fully Implemented and Maintained	Access Control	*DHSCAT-2.15.5*	*Maintained at the firewall level and on each endpoint.*
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	An operator attempts to connect to a known hacking website. The connection is blocked. The operator and IT are notified of the attempt.	1	Fully Implemented and Maintained	Access Control	*ISA62443-3-3.9.3, NIST800-53.F-SC.SC-7, NIST800-82.5.6*	*Maintained at the firewall level and on each endpoint.*
IA-3	Role based access control system established including policies and procedures.	SCADA software implements unique usernames and passwords with different levels of control based on roles.	1	Fully Implemented and Maintained	Access Control	*DHSCAT-2.15, NIST800-53.F-AC.AC-3*	*Domain-User access control established for each account. No Guest access allowed on corporate network.*
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).	Defined clearance requirements for individuals to access confidential information.	1	Fully Implemented and Maintained	Access Control	*DHSCAT-2.5.5, NIST800-53.F-AC.AC-3*	*Access to confidential data is controlled through user permissions granted vial Active Directory.*
IA-5	Access control for diagnostic tools and resources and configuration ports.	PLC programming software is only available at select workstations and only accessible to SCADA technicians.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.13.1.1, NIST800-53.F-AC.AC-3*	*Access to SCADA and IT files are limited to specific members of the IT and OM departments.*
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Contracts with third-party equipment vendors establish security requirements for remote access to equipment.	1	Fully Implemented and Maintained	Access Control	*NIST800-53.F-AC.AC-17, NIST800-82.5.15*	*Access by support vendors with SLAs is limited to each particular vendor's equipment/systems .*
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.	To use the plant guest network, users are required to accept a user agreement.	1	Fully Implemented and Maintained	Access Control	*DHSCAT-2.15.26, DHSDID-3, ISA62443-3-3.5.8*	*WIFI Guest network framework configured, managed, and maintained.*
IA-9	Multifactor authentication system established for critical areas.	Remote access to the SCADA system requires two factor-authentication.	1	Fully Implemented and Maintained	Access Control	*ISA62443-1-1.5.3, ISA62443-3-3.5.3, NIST800-34.3.2, NIST800-82.6.2.7*	*Certificate 2FA and email 2FA in place*
PE-1	Security perimeters, card controlled gates, manned booths, and procedures for entry control.	Personnel are required to present a badge to access the PCS.	1	Fully Implemented and Maintained	Physical Security	*DHSCAT-2.4.3, ISOIEC27.27001.AA.A.11.1.1, NIST800-53.F-PE.PE-3*	*PCS network operating centers are key controlled*
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Access to the server room is restricted to authorized staff only.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.11.1, NIST800-53.F-PE.PE-5*	*PCS network operating centers are key controlled*
PE-3	Physical security and procedures for offices, rooms, and facilities.	Staff lock doors that allow access to PCS assets. Security guards inspect doors to make sure they are locked property.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.11.1.3, NIST800-53.F-PE.PE-4*	*Physical security and access control in in place on all facilities with intrusion alarms with active monitoring*
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Fire suppression unit installed around critical equipment.	1	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.4, ISOIEC27.27001.AA.A.11.1.4, NIST800-53.F-CP.CP-2*	*Data operations centers are fully redundant with generator and UPS backup power.*
PE-5	Physical security and procedures for working in secure areas.	Documentation for physical security procedures is included with new employee training and reviewed at regular training events.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.11.1.5, NIST800-53.F-PE.PE-1*	*Data operating centers are key controlled*

PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from IT/PCS areas.	Server room and PLC cabinets are isolated from areas that delivery personnel and customers may visit.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.11.1.6, NIST800-53.F-PE.PE-16*	*Access control is in place for all Industrial Control Systems, Data and Network operation centers.*
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	The utility monitors facilities using security cameras.	1	Fully Implemented and Maintained	Physical Security	*DHSCAT-2.4, ISOIEC27.27001.AA.A.11.1.4, NIST800-53.F-CP.CP-7*	*Physical security and access control in in place on all facilities with intrusion alarms with active monitoring*
PE-8	Physical/logical protection against power failure of equipment (UPS).	Uninterruptible power supplies (UPS) are available as power backup for critical components.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.11.2.2, NIST800-53.F-CP.CP-8*	*All critical IT and SCADA equipment is power redundant equipped with UPS and/or generators.*
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	A utility has a standby power source with separated power cabling for critical sites.	1	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.11.2.3, NIST800-53.F-PE.PE-9*	*All critical IT and SCADA equipment is power redundant equipped with UPS and/or generators.*
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communication.	1	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.8.11, ISA62443-3-3.9, NIST800-82.6.2.16.1*	*Cryptographic keys are maintained for VPN access to internal networks and servers.*
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).	A water utility chooses to not allow personal mobile devices to connect to the control network. The utility does provide mobile devices managed by IT that can connect to the network.	1	Fully Implemented and Maintained	Server and Workstation Hardening	*NIST800-28.5, NIST800-34.3*	*Connection to the network is limited to district owned, tablets and phones and these IOS and Android devices are managed through a District approved Mobile Device Management (MDM) platform. Active Threat Hunting NGAV installed on all server and workstation platforms.*
SC-12	Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.	Remote access to the SCADA system requires two factor-authentication.	1	Fully Implemented and Maintained	Access Control	*NIST800-53.F-AC.AC-17*	*MFA required for access to all OT/SCADA infrastructure.*
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	An actively managed firewall is in place to allow secure data transfer via DMZ.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.5.1*	*Deep packet inspection enabled on all internet communiques.*
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.5.4*	*CVEs and malware definitions are automatically updated as new threats and vulnerabilities arise. Access in/out of external firewall is monitored and limited.*
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	A utility employs multiple types of physical and cybersecurity efforts to protect assets and systems. The efforts include such things as locking doors, physical access control, and unique login requirements for each staff member.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.5.5*	*MFA, Threat Hunting, NGFW, ACLs, IPS, IDS all implemented*
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Within the SCADA system network, vendor systems are on a separate subnet.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.6.2.1.3*	*SCADA network are on separate VLANs*
SC-18	Minimize wireless network coverage.	Tests are conducted regularly to determine if the WiFi signals reach outside the intended area of use. If the signal reaches outside the intended area, the signal is turned down accordingly.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.6.2.1.5*	*Wifi signal power settings are configured for limited access range.*
SC-19	802.1X user authentication on wireless networks.	No "open" WiFi connections are allowed.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.6.2.1.5*	*WPA-2 used (applicable to Camrosa Guest Wifi network only)*

SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Operators have one username and password for PCS equipment which is managed from a central system.	1	Fully Implemented and Maintained	Access Control	*DHSCAT-2.15.16*	*All corporate system assets are SSO except the billing system.*
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.	WiFi equipment in the plant does not connect directly to SCADA network.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.6.2.1.5*	*There is no wifi available/allowed for connection to internal OT SCADA networks.*
SC-21	Unique wireless network indentifier (SSID) for control network.	The WiFi for the control system has a unique SSID from the business network.	1	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-82.6.2.1.5*	*SSID are unique and hidden*
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	A wireless LAN specific domain controller is in place.	1	Not Planned and/or Not Implemented - Risk Accepted	Telecommunications, Network Security, and Architecture	*NIST800-82.6.2.1.5*	*NON-APPLICABLE. Camrosa is deprecating the use of wifi for access to internal networks. Guest network access is separate/divorced from internal networks.*
SC-23	Wireless communications links encrypted.	All data transferred via the wireless network is encrypted using current wireless communication best practices.	1	Fully Implemented and Maintained	Encryption	*NIST800-82.6.2.1.5*	*WPA-2 used (applicable to Camrosa Guest Wifi network only)*
SC-24	Communications links encrypted.	All data transferred via the wired network is encrypted using current wired communication best practices.	1	Fully Implemented and Maintained	Encryption	*NIST800-82.6.2.1.5*	*Latest revisions of Transport Layer Security are fully implemented*
SC-25	Virtual Private Network (VPN) using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	An operator who can access the system remotely must do so through a secured VPN client configuration.	1	Fully Implemented and Maintained	Encryption	*NIST800-82.5.10.2, NIST800-82.5.4*	*MFA through secure VPN is fully implemented*
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.	All external communication with the PCS is implemented via DMZ.	1	Fully Implemented and Maintained	Governance and Risk Management	*ISA62443-3-3.9.2, NIST800-82.5.5.4*	*Corporate networks are segmented to maximize security.*
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and non-repudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.	The company selected to perform billing is compliant with pertinent laws, regulations, policies, procedures that are relevant to the utility.	1	Fully Implemented and Maintained	Governance and Risk Management	*NIST800-53.F-AU.AU-10*	*It is the policy of the District not to store or transmit customer credit card information on any internal or external District information system. This includes public facing websites owned or operated by the District. However, the District does contract with third-party credit card processing firms which may store or transmit customer credit card information (e.g., online bill pay) and these entities must comply with all regulations dealing with security of customer information, including, but not limited to:* *• Payment Card Industry Data Security Standard (PCI DSS)* *• Any other applicable security policies of the Camrosa Water District*
SI-3	Interactive system for managing password implemented to ensure password strength.	When configuring a new user's password, it must meet minimum character length requirements.	1	Fully Implemented and Maintained	Access Control	*NIST800-53.F-IA.IA-5*	*Group policy in place to ensure sufficient password strength, complexity and periodic update.*
AT-1	A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures.	An operator finds a USB media device. Based on their cybersecurity training, they know not to use it on the company network.	2	Fully Implemented and Maintained	Education	*DHSCAT-2.11, ISA62443-2-1.A.3.2.4*	*Acceptable Use policy in place for proper use of network resources. Users are trained on cyber security topics monthly.*
AT-2	Job specific security training including incident response training for employees, contractors and third party users.	An operator has received what they believe to be a malicious email. They recognize that it is a phishing attack based on security training awareness programs the company has in place.	2	Fully Implemented and Maintained	Education	*AWWAG430.4.3, DHSCAT-2.11.3*	*Monthly cyber security awareness training on such topics as phishing and social engineering are provided along with testing.*

AU-5	Risk based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of policies and plans throughout the organization. Another purpose of the framework is to ensure consistency across plans in terms of priorities, contact data, testing, and maintenance.	The facility has a documented and tested contingency plan to operate the facility without the use of SCADA software, in the case of attack by ransomware.	2	Partially Implemented	Business Continuity and Disaster Recovery	*DHSCAT-2.12.2, ISA62443-2-1.A.3.2.5, ISOIEC27.27003.8.2, NIST800-34.WD*	*Business Continuity is currently addressed with local and cloud based backups, clustered fault tolerant application servers and cloud based Disaster Recovery services. Full policy development for Business Continuity planning is scheduled for FY-23.*
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	The business continuity plan is revised annually. Revisions are informed by planned exercises, actual events, or documented changes.	2	Planned and Not Implemented	Governance and Risk Management	*NIST800-124.2.2.1-5, NIST800-34.WD*	*Policy development for Business Continuity planning is scheduled for FY-23.*
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	The PCS has a testing/development environment to allow changes to be implemented without immediate effects to the production environment.	2	Fully Implemented and Maintained	Business Continuity and Disaster Recovery	*ISOIEC27.27001.AA.A.14.2.9, NIST800-34.WD*	*The District's IT Procurement, Acquisition, and Support policy addresses the need that careful consideration be given in the procurement and acquisition of new IT systems to control costs, ensure compatibility, future supportability, and determine the impacts and risks these new systems may have to cyber security.*
CM-3	Separation of duties implemented for user processes including risk of abuse.	Operators are only given clearance to areas they are expected to work in. Supervisors have the ability and training to monitor SCADA tech activities in the PCS.	2	Fully Implemented and Maintained	Application Security	*ISA62443-2-1.A.3.3.5.3, ISOIEC27.27001.AA.A.6.1.2, NIST800-53.F-AC.AC-5*	*Per policy, separation of duties and auditing are implemented to mitigate the risk of abuse.*
CM-4	Separation of duties implemented for development, production, and testing work.	A SCADA technician must have a second technician review changes made to production equipment before they are implemented.	2	Fully Implemented and Maintained	Application Security	*ISOIEC27.27001.AA.A.6.1.2, NIST800-53.F-AC.AC-5*	*IT and OT (SCADA) development environments are separate from production environments.*
CM-5	SLAs for all third parties established, including levels of service and change controls.	A security policy that outlines what access permissions are distributed to third party employees.	2	Fully Implemented and Maintained	Service Level Agreements (SLA)	*DHSCAT-2.5.9, NIST800-53.F-SA.SA-9*	*Per policy, SLAs for all third party vendors will clearly define the roles, responsibilities, service scope and performance standards of both parties and also include:* *• Availability & uptime guarantee* *• Escalation procedures* *• Data center redundancy and/or cloud-to-cloud backup plan* *• Computing performance specifications* *• Exit strategy*
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.	IT monitors SCADA computers for processor usage that could indicate cryptojacking activity.	2	Fully Implemented and Maintained	Service Level Agreements (SLA)	*DHSDID-3.4, NIST800-53.F-CM.CM-11*	*SNMP monitoring and Intrusion Detection alerts configured on 100% of network, server and workstation assets*
IR-1	Incident response program established with a formal Emergency Response Plan to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events. Exercises conducted to test and revise plans and build organizational response capabilities.	Emergency Response Plan includes procedures for recovering SCADA system operation from system backup.	2	Fully Implemented and Maintained	Governance and Risk Management	*AWWAG430.4.11, DHSCAT-2.12.16, NIST800-61R2.WD*	*Per policy, Recover Time Objective (RTO) and Recover Point Objectives (RPO) have been established for single and multiple entity recoveries. Formal Emergency Response Plans are in place.*
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	The condition of offsite equipment and risk factors acting on the equipment are periodically reviewed and assessed via an independent party.	2	Planned and Not Implemented	Governance and Risk Management	*ISOIEC27.27001.AA.A.11.2.6, NIST800-53.F-SA.SA-9*	*Instead of an off-site equipment program, the District relies on fully redundant off-site Network/Data centers that can operate, fully functional stand-alone.*

PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.	A utility has a network intrusion detection system (NIDS) to monitor network traffic.	2	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	ISOIEC27.27002.15.3, NIST800-53.F-AU.AU-6	See Camrosa IT Plan, Section 3.9 Log Management Policy for more detail
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	Third parties must review and sign an information exchange policy before connecting to the system.	2	Fully Implemented and Maintained	Service Level Agreements (SLA)	ISOIEC27.27001.AA.A.6.2.3, NIST800-124.4.1, NIST800-53.F-SA.SA-9	See Camrosa IT Plan, § 2.3.1 New System Implementation and Support, 3.7 Security Incident Management Policy, 3.15 Cloud Computing Policy for more information
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	A third-party system integrator would need to contact IT before connecting to the system's network.	2	Fully Implemented and Maintained	Governance and Risk Management	NIST800-53.F-SI.SI-5	See Camrosa IT Plan § 3.10 Safeguarding Customer Information Policy, 3.18 Vulnerability Assessment Policy for more information
RA-2	Third party agreement process to ensure that external vendors and contractors utilize appropriate security measures for access, processing, communicating, or managing the organization's information or facilities.	System integrators can only access the facility's equipment remotely from a VPN connection.	2	Fully Implemented and Maintained	Governance and Risk Management	NIST800-53.2.5, NIST800-53.F-SA.SA-9	See Camrosa IT Plan, § 2.3.1 New System Implementation and Support, 3.7 Security Incident Management Policy, 3.15 Cloud Computing Policy for more information
SC-10	Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).	Ports are disabled for all network devices when not in use.	2	Fully Implemented and Maintained	Server and Workstation Hardening	NIST800-34.3.2, NIST800-53.F-CM.CM-6	See Camrosa IT Plan, § 3.5 Firewall Policy, 3.16 Server Security Policy, 3.20 Workstation Configuration Security Policy, 3.21 Wireless (WiFi) Connectivity Policy for more information.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Organization has a FAT procedure that requires vendors to demonstrate security of systems before they are purchased.	2	Planned and Not Implemented	Governance and Risk Management	NIST800-53.F-SA.SA-11	* Requires further consultation with District's IT/OT MSP for plan formulation.
SC-4	Intrusion detection, prevention, and recovery systems including approved policies and procedures established to protect against cyber-attacks. System includes repository of fault logging, analysis, and appropriate actions taken.	Monitoring of IDS is conducted to determine if ongoing attacks are occurring and incidence response actions have been documented.	2	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	NIST800-53.F-SI.SI-4	See Camrosa IT Plan, § 3.5 Firewall Policy, 3.16 Server Security Policy, 3.20 Workstation Configuration Security Policy, 3.21 Wireless (WiFi) Connectivity Policy for more information.
SC-5	Anomaly based IDS/IPS established including policies and procedures.	The IT tech monitors IDS system exception logs daily to determine if ongoing attacks are occurring and works with SCADA tech to address any issues.	2	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	NIST800-53.F-SI.SI-4	See Camrosa IT Plan, § 3.5 Firewall Policy, 3.16 Server Security Policy, 3.20 Workstation Configuration Security Policy, 3.21 Wireless (WiFi) Connectivity Policy for more information.
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.	2	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	NIST800-82.5.6	See Camrosa IT Plan, § 3.5 Firewall Policy, 3.16 Server Security Policy, 3.20 Workstation Configuration Security Policy, 3.21 Wireless (WiFi) Connectivity Policy for more information.
SC-7	Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures.	Web applications for SCADA software use encryption to protect data in transit.	2	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	DHSCAT-2.9.5, NIST800-53.F-AC.AC-21	See Camrosa IT Plan, § 3.10 Safeguarding Customer Information Policy, 3.11 Network Security and Virtual Private Network (VPN) Acceptable Use Policy, 3.12 Bring Your Own Device (BYOD) Policy, 3.15 Cloud Computing Policy, 3.21 Wireless (WiFi) Connectivity Policy for more information.
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.	Within the SCADA system network, vendor systems are placed on a separate subnet rather than being on a single "flat" network.	2	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	DHSDID-3.1.1, ISA62443-1-1.5.8, ISA62443-3-3.9.3, NIST800-82.5.4	See Camrosa IT Plan, Section 3.5 Firewall Policy for more information.

SC-9	Process isolation established to provide a manual override "air gap" between highly sensitive systems and regular environments.	A manual method for disconnecting the ICS network from other networks is implemented and documented.	2	Fully Implemented and Maintained	Operations Security	*ISA62443-3-3.9.3.3*	*OT SCADA and IT Financial Systems are segmented on separate VLANs. With ACLs in place to limit inbound/outbound traffic. Air-gapping/manual override is simplified requiring single disconnect from out firewall.*
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.	Acquired assets are inspected, assessed, and documented before implementation with existing systems.	2	Planned and Not Implemented	Governance and Risk Management	*DHSCAT-2.5, ISOIEC27.27001.AA.A.14.2.9*	** Requires further consultation with District's IT/OT MSP for plan formulation.*
SI-5	Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as IT audit tools that can modify or delete audit data.	Utility has implemented tiered access so non-administrator users are unable to make changes to system security settings.	2	Fully Implemented and Maintained	Application Security	*DHSDID-3.5.1, NIST800-53.F-IA.IA-2*	*Powershell disabled on all servers and workstations by default. Also see Camrosa IT Plan, Section 3.2 User Account/Password Management Policy for more information.*
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Reviews of the organization's confidentiality/non-disclosure agreements are periodically scheduled by a responsible party.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.13.2.4*	*See Camrosa IT Plan, Appendix A, Receipt of Acceptable Use of the Camrosa Water District's Information Systems.*
CIE-1	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threat throughout the engineering life-cycle including: design, implementation, maintenance, and decommissioning.	Engineering staff is fully aware of the potential for a cyber breach. They design electrical and mechanical systems to provide functionality in the case of a SCADA system compromise.	3	Planned and Not Implemented	Cyber-Informed Engineering	*CCE-CIE*	*Since CIE is a recently developed methodology that looks holistically over the engineering life cycle in order to reduce cyber risks, the District is still evaluating practical controls that can be put in place to address CIE.*
CM-1	Policies for defining business requirements including data validation and message authenticity established to ensure that new/upgraded systems contain appropriate security requirements and controls.	Policies to define minimum security features (i.e. secure protocols, active directory integration, etc.) required for new systems. This could include review and approval by change management and/or security team.	3	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.15.28, ISA62443-1-1.5.5*	*See Camrosa IT Plan, Section 2, Information Technology Procurement, Acquisition, and Support Policy for more information regarding onboarding of new/upgraded systems.*
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.	The Emergency Response Plan is stored in a central repository and clearly displays the version and date of when it was implemented.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.5.1.2, NIST800-53.G.PM-1*	*Cyber policies are reviewed annually for alignment with current standards.*
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	An operator misplaces a managed phone. Based on the missing equipment policy, they contact IT to report the device lost.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.11.2.1, NIST800-53.F-PE.PE-15*	*Per policy, the District maintains asset inventory lists of desktop, server, and infrastructure hardware and software. See Camrosa IT Plan § 3.10 Safeguarding Customer Information Policy, and 3.16 Hardware and Electronic Media Disposal Policy for more information.*
IR-3	A legal/contractual/regulatory framework established with a formal Emergency Response Plan to track legal/contractual/regulatory requirements and the efforts to meet them with respect to each important system within the organization. Another purpose of the framework is to ensure compliance of policies and procedures with privacy laws, handling cryptographic products, intellectual property rights, and data retention requirements.	The Emergency Response Plan is reviewed and updated once a year by responsible staff.	3	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.9.7*	*Risk & Resiliency Assessment updated 6/28/2021 Emergency Responze Plan was last updated 12/17/2021*
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	An approved data leakage prevention (DLP) system is implemented or manual procedures to control data and/or software leaving organization.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.8.3.1, NIST800-53.F-MP.MP-1*	*Policies and controls are in place to monitor and control exfiltration of data through email, file transfer, etc.*

PM-1	An asset inventory of all electronic components including model, software / firmware, etc. that is maintained and referenced when vendor vulnerabilities are disclosed.	A database is used to keep track of building conditions in the facility.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISA62443-3-3.11.1, ISOIEC27.27001.AA.A.8, NIST800-53.F-CM.CM-8, NIST800-53.F-CM.CM-9*	*Per policy, the District maintains asset inventory lists of desktop, server, and infrastructure hardware and software. See Camrosa IT Plan § 3.10 Safeguarding Customer Information Policy, and 3.16 Hardware and Electronic Media Disposal Policy for more information.*
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	PLCs that cannot update past a specific security revision are not acceptable for use in the PCS.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.8.1.1, NIST800-53.G.PM-5*	*See Camrosa IT Plan, Section 3.1 Acceptable Use of Information Systems Policy for more information.*
PS-1	Policies and procedures for hiring/terminating processes on employees, contractors, or support companies to include background checks and contract agreements approved and implemented.	A background check on employees is required before they may be given access to the PCS system.	3	Fully Implemented and Maintained	Personnel Security	*DHSCAT-2.3.1*	*Per policy; new employee onboarding training, orientation, and instruction are provided. Cyber controls for terminating access are in place.*
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third party users.	A company policy is in place limiting the access of third-party users to assets, systems, and data.	3	Fully Implemented and Maintained	Personnel Security	*DHSCAT-2.3.9*	*Per policy, the roles and associated duties of each member of the IT Department are clearly defined along with their levels of network access.*
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.	Confidential documents are stored in locked file cabinets when not in use, as required by policy.	3	Fully Implemented and Maintained	Personnel Security	*DHSCAT-2.3.8, ISOIEC27.27001.AA.A.11.2.9, ISOIEC27.27002.11.2.9*	*See Camrosa IT Plan, Section 3.10 Safeguarding Customer Information Policy for more information on the District's Clean Desk policy.*
PS-4	Disciplinary process for security violations established.	An operator who props open doors to critical areas could face disciplinary action as outlined in the utility's policies and procedures.	3	Fully Implemented and Maintained	Personnel Security	*DHSCAT-2.3.8, ISA62443-2-1.A.3.3.2, ISOIEC27.27001.AA.A.7.2.3*	*Per policy, Any breach of the Acceptable Use policy by the employee may result in disciplinary action, up to and including termination of employment.*
SA-1	Authorization process established for new systems or changes to existing information processing systems.	A change management/review process is used to evaluate suggested changes to facility.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.14.2, NIST800-53.G.PM-10*	*See Camrosa IT Plan, Section 2, Information Technology Procurement, Acquisition, and Support Policy for more information regarding established authorization process new systems or changes to existing IPS.*
SA-2	Change controls of systems development, outsourced development, system modification, and testing established, including acceptance criteria for new systems, monitoring of internal/outsourced development, and control of system upgrades.	A third-party system integrator is preparing to make changes to SCADA software. The SCADA tech requires the integrator to follow the change procedure and test the changes in a sandbox environment before they are deployed in production.	3	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.6.3, ISOIEC27.27001.AA.A.14.2.2, NIST800-53.F-SA.SA-10*	*See Camrosa IT Plan, Section 2, Information Technology Procurement, Acquisition, and Support Policy for more information regarding system change controls.*
SA-3	Change controls of operating systems, network configuration/topology, network security established, including changes to IDS/IPS, traffic control/monitoring, new systems, and system upgrades.	Automatic updates to the operating system are disabled, but monthly manual updates are reviewed and applied in coordination with operations.	3	Fully Implemented and Maintained	Governance and Risk Management	*NIST800-82.6.2.5*	*See Camrosa IT Plan, Section 2, Information Technology Procurement, Acquisition, and Support Policy for more information regarding system change controls.*
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.	Remote access is restricted to only the most necessary applications and only allowed through secure measures.	3	Fully Implemented and Maintained	Operations Security	*DHSCAT-2.15.25, NIST800-34.ES*	*Per policy, Mobile Device Management (MDM) with malware protection enabled for all District owned mobile devices.*
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	System backups are tested on a regular basis by completing a system restoration to the test environment.	3	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.14.2.3, NIST800-53.F-CM.CM-3*	*See Camrosa IT Plan, Section 3.23 Data Backup and Recovery Policy for more information.*
SI-4	Organization-wide clock synchronization system in place.	All managed network devices synchronize their clocks to a known good source.	3	Fully Implemented and Maintained	Telecommunications, Network Security, and Architecture	*NIST800-53.F-AU.AU-8*	*Camrosa domain synchronized to Stratum-1, NTP timing.*
SU-1	A supply chain risk management program.	Chain of custody documentation is required for all chemicals used in treatment.	3	Planned and Not Implemented	Governance and Risk Management	*NIST-CSF v1.1*	

CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Inviting all affected parties to discussions to prevent the development of vulnerabilities in the facility.	4	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.14.2.2, NIST800-53.F-CM.CM-1*	*As part of the change process of any IT system or sub-system, the District consults all stakeholders including Management, IT, Operations, and system users.*
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.	Upon staff termination or resignation, login credentials are disabled as part of the Human Resources process.	4	Fully Implemented and Maintained	Access Control	*ISOIEC27.27001.AA.A.9.2.1, NIST800-53.F-IA.IA-4*	*Auditing and reporting of user accounts is performed quarterly by the District IT/OT Managed Service Provider*
IR-2	A security program established with a formal Emergency Response Plan to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.	A SCADA tech believes a machine is infected and responds according to the utility's emergency response plan for cybersecurity based incidents.	4	Fully Implemented and Maintained	Governance and Risk Management	*AWWAG430.4.4, DHSCAT-2.12, NIST800-61R2.WD*	*A formal Emergency Response Plan and Incident Response Plan are in place.*
MA-1	A controlled maintenance system is in place to organize, schedule, document, and monitor the maintenance and repairs performed on information system assets in the PCS.	Based on the company's controlled maintenance program, a utility will format network devices to factory settings before sending them out of the organization for maintenance.	4	Not Planned and/or Not Implemented - Risk Accepted	Service Level Agreements (SLA)	*ISOIEC27.27001.AA.A.11.2.4, NIST800-53.F-MA.MA-2*	*The District performs necessary repairs to IT recordable media in-house. This control ID is non-applicable.*
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.	The utility is a member of DHS's CISA mailing list to receive frequent communications on PCS vulnerabilities discovered and patches available. SCADA techs regularly review alerts to determine if the alerts are applicable to their system.	4	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.13.2.4, NIST800-53.F-AC.AC-19*	*Currently engaged with CISA for weekly Cyber Hygiene vulnerablity and PEN testing and Web Application Scanning (WAS) of all internet facing IP addresses.*
MP-1	Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).	When decommissioning a network device that was used in the production environment, IT is required to return it to factory conditions before it leaves the facility.	4	Fully Implemented and Maintained	Governance and Risk Management	*DHSCAT-2.13, NIST800-53.F-MP.MP-6*	*See Camrosa IT Plan, Section 3.6 Hardware and Electronic Media Disposal Policy for more information.*
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Company policies and procedures are available in a central, secure, shared location.	4	Fully Implemented and Maintained	Governance and Risk Management	*ISA62443-2-1.A.3.2.6, NIST800-53.G.PM-1*	*All policies and procedures are available to all staff on the District's intranet website.*
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	A policy to store and manage access to PLC programs.	4	Fully Implemented and Maintained	Governance and Risk Management	*ISOIEC27.27001.AA.A.8.2.1, NIST800-53.F-RA.RA-2*	*Sensitive IT and OT (SCADA) data repositories are under controlled access and available only to necessary IT and OT personnel.*
SU-2	A supply chain risk management program that includes cybersecurity.	Preferred vendors for computer hardware, software and peripherals are identified and selected based on evaluation of their supply chain	4	Fully Implemented and Maintained	Governance and Risk Management	*NIST-CSF v1.1*	*Per policy, preferred IT/OT vendor lists are maintained.*

Continue to Tab 3 RRA-Control Status Summary

The **RRA-Control Status Summary** tab includes two tables. The first summarizes the recommended controls' status by priority. This is shown in a "heat map" format to visually indicate the number of controls of various priority and their associated status. Additional details on the status categories are provided following the table.

The second table identifies the number of controls associated with each improvement project categories as identified in the guidance document. These projects account for recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented" on the RRA-Control Output tab.

Please note: Recommended controls that are not fully implemented should have a plan for implementation or the risk must be accepted. When used in this manner, this output may become the initial phase of an implementation plan. In addition, controls identified with a status of "Controls Planned and Not Implemented" or "Controls Partially Implemented" may be included as "strategies and resources to improve the resilience of the system..." in an AWIA-compliant ERP.

Control Status Summary:

The second table summarizes the user defined implementation status of the recommended controls from the RRA- Control Output tab. The colors provide a visual indication the recommended controls with the associated status.

	Total Controls Not Fully Implemented	Not Planned and/or Not Implemented - Risk Accepted	Controls Planned and Not Implemented	Controls Partially Implemented	Controls Fully Implemented and Maintained
Priority 1 Controls	0	2	0	0	43
Priority 2 Controls	5	0	4	1	20
Priority 3 Controls	2	0	2	0	18
Priority 4 Controls	0	1	0	0	8

% of Recommended Controls Currently "Fully Implemented and Maintained":	90	%
% Recommended Controls that are "Partially Implemented" or "Planned and not Implemented":	7	%
% Recommended Controls that are "Not Planned and/or Not Implemented - Risk Accepted":	3	%
Controls Missing Implementation Status:	0	

Not Planned and/or Not Implemented – Risk Accepted	The controls are not currently implemented or planned for implementation. The organization accepts risks associated with the controls not being implemented.
Planned and Not Implemented	Priority 1 or Priority 2 controls that have not been implemented; however, implementation of the controls are planned.
Planned and Not Implemented/ Partially	Priority 1 or Priority 2 controls that are partially implemented by internal or external resources. Priority 3 or Priority 4 controls that are neither planned nor implemented.
Partially Implemented –	Priority 3 or Priority 4 controls that are partially implemented by internal or external resources.
Fully Implemented and Maintained –	The controls are fully implemented and actively maintained by internal or external resources.

Date of Tool Usage:
Utility/Facility/System:

Attendees - Names/Roles:
Tool Version:

Cyber Risk Management Improvement Projects

Projects by total number of controls

Project Number	**Improvement Project**	**Number of controls project addresses**
1	Governance and Risk Management Improvements Projects	5
2	Business Continuity and Disaster Recovery Improvements Projects	1
3	Server and Workstation Hardening Improvements Projects	0
4	Access Control Improvements Projects	0
5	Application Security Improvements Projects	0
6	Encryption Improvements Projects	0
7	Data Security Improvements Projects	0
8	Telecommunications, Network Security, and Architecture Improvements Project	0
9	Physical Security of PCS Equipment Improvements Projects	0
10	Service Level Agreements (SLA) Improvements Projects	0
11	Operations Security (OPSEC) Improvements Projects	0
12	Cyber-Informed Engineering Improvements Projects	1
13	Education Improvements Projects	0
14	Personnel Security Improvements Projects	0

Continue to Tab 4 ERP-Improvement Projects

Date of Tool Usage:
Utility/Facility/System:

Attendees - Names/Roles:
Tool Version: