CYBERSECURITY AND DISASTER RECOVERY WORKSHOP

WORKBOOK

2025

NCSC
National Center for State Courts

Cybersecurity and Disaster Recovery Workshop

Workbook and Templates

Acknowledgments

The Court Cybersecurity and Disaster Recovery Regional Workshop was funded by a strategic initiative grant (SJI-24P003) awarded by the State Justice Institute (SJI). The National Center for State Courts (NCSC) would like to thank SJI and the following participating organizations and contributors for their work on the Cybersecurity and Disaster Recovery Workshop series.

Participating Organizations

- Center for Internet Security (CIS)
- Joint Technology Committee (JTC)
- Conference of Chief Justices (CCJ)
- Conference of State Court Administrators (COSCA)
- Court Information Technology Officers Consortium (CITOC)

Contributors

- Jannet Okazaki, NCSC
- Shay Cleary, NCSC
- Justin Mammen, NCSC
- Tim Holthoff, AR Courts
- Michelle Nolan, CIS
- Brian de Vallance, CIS
- Carlos Kizzee, CIS
- Matt Cowles, CSG
- Jim Harris, NCSC
- Nathan Hall, NCSC
- Katana Evans, NCSC

The content is solely the responsibility of the contributors and does not necessarily represent the official views of the SJI and any participating organizations.

Table of Contents

Instructions

Overview

This document will help prepare participants for the Cybersecurity and Disaster Recovery Workshop. It is crucial that participants carefully review the information included in this document and complete it, including tables and activities, before the in-person workshop.

The workshop instructors refer to these activities as “Blue Sky” work. “Blue Sky” days are an opportunity to dedicate some time and resources needed to develop a cyber response plan when not under the pressure of an actual incident. Ultimately, a “Gray Sky” day will come when an event such as a ransomware message appears on a court computer, your security monitoring systems detect unauthorized access, or your case management systems become inaccessible. In those “Gray Sky” days of an actual cyber incident, you and your leadership team will more than likely be overwhelmed and in a position to play catch up to respond to the incident. Phones will ring incessantly, you may be cut off from email, and time-sensitive decisions will need to be made with limited to no information. This “Blue Sky” work should improve your court’s resiliency and help prepare you for the in-person cybersecurity workshop.

The sample templates in this workbook (Tables 1-9) should only be used for guidance. The blank templates are in the appendices (Appendix A-I).

Section 1 – Team Directories

If the court already has an Emergency Operations Plan/Occupant Emergency Plan or a Continuity of Operations Plan, a Crisis Management Team (CMT) may already be identified. If not, this is where the court will establish the leadership team needed to be assembled in a crisis.

The CMT should function as an overarching policy/executive body that governs and directs policy related to crisis response for the court. It serves as a decision-making authority that helps to direct priorities during a cyber incident. This group makes major policy decisions such as deciding when to send court staff home, determining court-wide communications, providing the court's statement to the media, etc. The CMT should consist of senior leadership such as the Presiding or Chief Judge, Chief Officers, General Counsel, Facilities Director, Public Information Officer, Emergency Management, and Lead Security Personnel (e.g., Sheriff Captain, Commander, etc.)

In cyber incidents, contingent on the staffing/organization of the court system, it may also be helpful to consider a specialized supporting crisis team to address the technical issues in a cyber incident. For example, an IT Cyber Incident Response Team (CIRT) could assemble to provide the subject matter expertise and coordination to handle the "boots on the ground" IT cyber response. These could include determining how to shut down servers, liaising with justice partner/AOC IT staff, enabling/disabling email traffic, restoring data from backups, etc.

While the CMT focuses on the overall strategic decisions in a cyber crisis, the IT CIRT focuses on the tactical IT actions that need to be enacted.

See Table 1.1 and Table 1.2 for a sample template used to identify your CMT.

See Appendix A for the blank template.

Table 1.1 Crisis Management Team (CMT) Directory (Sample)

Name	Agency	Phone	Email
Chief Judge			
Court Administrator			
Chief Information Officer			
General Counsel			
HR Director			

Public Information Officer			
Operations Director			
Emergency Manager			

Table 1.2 IT Cyber Incident Response Team (CIRT) Directory (Sample)

Name	Agency	Phone	Email
IT Director			
Network Engineer			
End User Support Manager			
County IT Director			
AOC IT Liaison			

Section 2 – Physical Locations

This section identifies the **physical locations** from which the court system operates. During a disruption event, physical locations may be assessed and operations altered to allow missioncritical work to continue. A **physical location** is all **owned, government-provided, or leased** brick-and-mortar buildings where court operations occur.

Local court organizations may **list all** court physical locations. If you are a **statewide organization,** limit the locations to **AOC and Supreme Court buildings**.

See Table 2 for a sample template for identifying court physical locations.

See Appendix B for the blank template.

Table 2. Court Physical Locations (Sample)

Name of Facility	Address
Downtown Justice Center	123 Street Name, City Name, ST, 55555
Juvenile Justice Center	

Section 3 – Essential Functions

Essential functions are the core element of a court's **Continuity of Operations (COOP) Plan,** and this plan covers all hazards and events, including cyber security incidents. These functions are fundamental to supporting the community's safety and the court's mission, especially in times of crisis and with limited resources. Essential functions are often linked to what is statutorily required of the courts. Other functions are judged essential based on criteria such as their importance to the court's mission, their role in the continuity of government, and their necessity to the performance of essential functions by other departments or agencies.

There are likely many other functions that are all very important but may not necessarily be "essential" in a disaster or emergency. Knowing what is essential to the safety and security of a community is vital. If essential functions are not clearly identified, the court may become easily overwhelmed in a crisis, not knowing what is truly essential and what can be accomplished with limited resources. Thus, when selecting essential functions, the mantra is: **"If everything is important, then nothing is important."** This section is designed to help a court identify a list of its most time-critical and essential functions that cannot be left undone without running afoul of a statutory obligation or risking failure of its mission.

An essential function is defined as a court function that cannot be left undone for 30 days without risking failure to meet statutory/mandatory obligations, failure of mission, or loss of trust, respect, and funding.

See Table 3 to view examples of essential functions.

See Appendix B for the blank template. Please use the template in the workbook to list **four** essential organizational functions.

Table 3. Essential Function (Sample)

Essential Function	Description
Criminal Proceedings - Conduct misdemeanor and felony criminal arraignments according to state laws and regulations.	Criminal proceedings required to ensure due process of law and continuity of the criminal justice system.
Receive, process, adjudicated civil protection orders.	Domestic and civil proceedings required to meet the needs of the most vulnerable, such as those seeking protective orders.
Search Warrants	Search warrants issuance and revocation.

Section 4 – Business Impact Analysis

Courts should also identify the impact of the essential function that cannot be completed. This can be done by completing a Business Impact Analysis (BIA). The BIA should include a **Recovery Time Objective** (RTO) for each essential function. ***An RTO is defined as the time within the department in which the process must be restored after an emergency to avoid severe consequences.***

For the workshop, take the **four** essential functions identified in the **previous section** and **identify the impact** on your stakeholders if that function is not completed. Then determine the **Recovery Time Objective** for that essential function.

See Table 4 for a sample template for the business impact analysis of essential functions.

See Appendix C for the blank template.

Table 4. Business Impact Analysis of Essential Functions (Sample)

EF Number	EF Description	Impact if EF is not completed	Recovery Time Objective
1	Conduct misdemeanor and felony criminal arraignments according to state laws and regulations.	Violation of a person's statutory right to a speedy trial. In-custody defendant could be released if not arraigned timely.	48 hours
2	Receive, process, adjudicate civil protective orders.	Individuals at risk could be unprotected. Critical safety issue for those who need protection.	24 hours
3	Process (to include initiation and revocation) of emergency search warrants.	Community at risk if warrants are not issued. Likewise, innocent individuals could mistakenly be arrested if warrants are not correctly revoked in the system. Dangerous individuals may avoid capture.	24 hours

Section 5 – Identification of Business Processes

In this section, the specific activities and processes that allow essential functions to be maintained during an incident will be identified. This identification is completed by conducting a **Business Process Analysis** (BPA). ***The BPA is a systematic process that identifies and documents the activities and tasks that are associated with the court's essential functions.*** The analysis identifies the resources, space requirements, costs, interdependencies, workflow processes, and support functions that ensure the continued execution of the court's essential functions. A BPA on each of the **four** essential functions previously identified should be conducted to determine the following:

- **Recovery Time Objective -** How quickly does this essential function need to come back online (e.g., one day, three days, one week, one month, etc.)? Note: This information was already completed in the prior section, so it can be pulled from there.
- **Department/Person Responsible** – Which court department does this essential function fall under? In addition, which person will take the lead role to ensure the continuity of this essential function?
- **Key Staff/Personnel** – Who are the key staff/personnel needed to carry out this essential function?
- **Resources** – What equipment and supplies are necessary to accomplish the essential function? (e.g., court stamp/seal, laptops, etc.)
- **Work Location and Space Requirements** – What specific layout or room is needed to accomplish the essential function?
- **Supporting Activities** – What are the activities that need to occur to ensure successful completion of the essential function (e.g., Facilities setup of a courtroom)?
- **Internal Dependencies/Essential Records** – What critical case management systems, computer programs, databases, bank routing numbers, etc., are needed to accomplish this essential function?
- **External Dependencies/Essential Records** – What external justice partner IT applications/programs or services are needed to accomplish this essential function? (e.g., DMV interface, credit card processing system, criminal complaint from prosecutor's office)
- **Manual Workarounds** – Are there manual workarounds developed in the event critical IT systems supporting the essential function are not available?
- **Judicial Emergency Orders** – Can emergency orders from the State's court of last resort provide any assistance to suspend deadlines or extend timeframes for accomplishing the essential function?
- **Related Regulation** – What requires the court to perform the essential function? Cite the government section or penal code reference if known.

- **Telework** – Can the essential function be conducted remotely while adhering to proper cybersecurity best practices?

Completing the BPA provides context and key information to help management continue essential functions in a disaster or emergency. For the workshop, please complete a BPA for each of the **four** essential functions identified in the previous section.

See Table 5 for a sample template for the business process analysis of essential functions.

See Appendix D for the blank template.

Table 5. Business Process Analysis of Essential Functions (Sample)

Essential Function 1	Recovery Time Objective	Department Responsible	Key Staff
Conduct misdemeanor and felony criminal arraignments according to state laws and regulations	24 hours	Criminal Operations/Criminal Manager	1 Judge, 2 Clerks, 1 Court Reporter, 1 Interpreter per courtroom. Total of three courtrooms needed. 1 Criminal Operations Supervisor to oversee operations.
	Resources Needed		
	Court seal, US and State Flag, court stamps, judicial robe, headsets for interpreters.		
	Work Location & Space Requirements		
	Three courtroom sized spaces. 1-2 judicial chambers (can be shared between three judges), secure passageway and holding area for in custody inmates.		
	Supporting Activities		
	Receive criminal filing from prosecutor's office. Have in-custody inmate transported to courtroom. Interpreters on standby.		
	Internal Dependencies/Essential Records		
	Criminal Case Management System. Warrant Tracking System.		
	External Dependencies/Essential Records		
	Criminal complaint from prosecutor's office. Sheriff bailiff services. DMV records. State law enforcement database.		
	Manual Workarounds		
	Will need to manually receive complaint from prosecutor's office. Use manual criminal operations forms if case management system is non-operational.		
	Related Regulation		
	Government Section Code: 285b		
	Can an Emergency Order provide relief?	☒ Yes ☐ No Notes: EO from the court of last resort can provide relief to extend timeframe up to 14 more days.	

Can EF be done via telework?	☐ Yes ☒ No Notes: Not readily feasible unless remote appearance can be accomplished at jail.

Section 6 – Technology Priorities

Court technology is a critical component for the continued operation of the courts and the administration of justice. Technology infrastructure and systems may become crippled during a cyber or other disruptive incident. When conducting the business process analysis in the previous section, some technology resources were most likely identified. In this exercise, technology resources and priorities will be determined. For example, the court case management system and document images support the essential functions. These technology resources are often referenced as either **internal** or **external dependencies**. Ranking those applications with their recovery time objective will assist the IT department in knowing what the priority restorations are and where to divert limited resources during a crisis.

Courts must also consider the sequencing of how these steps come back online. If, for example, a case management system needs to be restored, servers and internet access will first need to be online. Thus, restoration order is a key determining factor when evaluating how quickly technology needs to be returned. The **order of restoration** applied to technology systems should be considered for all critical software applications and infrastructure (e.g., email, phones, servers, etc.). Like prior sections, the IT Recovery Time Objective (RTO) identifies the maximum time that IT systems can be down before severe consequences are experienced. An important question for the court to consider is, “How long can it afford to be in the dark? “

Another critical metric in managing expectations and response is defining a Recovery Point Objective (RPO). Some data loss can occur if IT services are interrupted before backups are updated. The RPO establishes the maximum age of the files recovered from backup storage that are necessary for operations to resume. For example, if the RPO is 24 hours, backups should be made at least once daily. This means that, in the event of a disaster, the court would potentially lose up to one day’s worth of data.

For the purposes of the cybersecurity workshop, please identify **eight** critical **IT applications** and **vital records.** Once those are determined, **prioritize the top five** for restoration during a cyber incident.

See Table 6 for a sample template for technology priorities.

See Appendix E for the blank template.

Table 6. Technology Priorities (Sample)

IT Application/ Vital Record	Priority in Cyber Event	IT Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Unit Responsible/ Point of Contact	Notes
Email	1	1 hour	24 hours prior	Cloud Applications Unit, Cloud Application Manager	Microsoft 365 cloud-based solution
Servers	2	1 hour	72 hours prior	Infrastructure Unit, Infrastructure Manager	Majority of servers are in Criminal courthouse
Criminal case management system	3	24 hours	72 hours prior	IT Application Unit, Application Manager	Cloud based
SharePoint	4	24 hours	24 hours prior	Network Unit, Network Administrator	Some case management files are linked to files located on cloud based SharePoint site.
VOIP Phones		48 hours	N/A		
Protective order database	5	48 hours	1 week prior	Criminal Operations, Criminal Manager	Relies on physical server at downtown courthouse
Payroll Information		1 week	1 month prior	Accounting, Accounting Manger	County maintains backup of court payroll for one pay period (two weeks)

Section 7 – Communication Modalities

The court should identify all available modalities of communication that can be used during a crisis. Cyber incidents can quickly disrupt normal communication pathways (e.g., email, VOIP phones, etc.). Thus, identifying all possible communication modalities and having a mix of redundant modalities should be considered so the court does not become overly dependent on just one or two forms of communication. A sample of these different options includes the following:

- Mass notification systems (Typically, these are third-party systems that provide rapid alerting too many individuals through a simultaneous email, phone call, and text

message. These systems are a way to quickly contact many individuals and take the place of older phone trees.)
- Court website
- Emergency phone message number (Number where judges/staff can call in to obtain recorded updates about the court's operational status.)
- Cloud-based websites (Locations where judges/staff can obtain information offsite in the event they cannot access the court's network.)
- Emergency conference lines (internal/external)
- Two-way radios
- Satellite phones
- Videoconference platforms
- Social media
- External facility signage
- Fax lines
- Building public address (PA) systems

For the purposes of the cybersecurity workshop, please identify **all communication** modalities, and identify the **top five** priorities. Once those are determined, prioritize the top five for use during a cyber incident.

See Table 7 for a sample template for communication modalities.

See Appendix F for the blank template.

7. Communication Modalities (Sample)

Communication System	Priority in Cyber Event	Where is system located?	Who has access?	Unit responsible?	Who can receive communications?
VOIP Phones		All workstations and courtrooms	All	N/A – all judges/staff have access to use phones	All judges/staff
Email	2	All workstations and courtrooms	All	N/A – all judges/staff have access to email	All judges/staff
Mobile Phones		Executive Management are issued Verizon mobile phones	Executive Management Only	Facilities department responsible for maintaining mobile phone contract	No restrictions on where calls can go to. Phones can be used as mobile hotspots if needed.

Table

Mass Communication (Ready Court)	1	Cloud based system	Court Emergency Manager, Court Administrator, HR Dir., Facility Dir.	IT Director oversees contract with third party vendor.	All judges/staff. Some key stakeholders (e.g., prosecutor, public defender, probation).
Two-Way Radios		Evacuation leaders at all courthouses and CMT	Evacuation leaders at all courthouses and CMT.	Court Emergency Manager	Only those who have a radio (Court uses Channel 1, Sheriff uses Channel 2).
Emergency Phone Message Number	3	Hosted on a third-party server (number is XXX-XXXXXXX)		IT Director or HR Director can leave messages on this line.	All judges/staff
Cloud based information site	5	Secure online SharePoint site https://secure...	IT Director, HR Director	Court PIO will post updates on at the direction of the CMT	All judges/staff
Videoconference Platforms	4	Microsoft Teams, Cisco WebEx	All judges/staff	IT Director	All judges/staff
Satellite Phones		One phone located at each courthouse in the Facilities Office	Facility Manager	IT Director	No restrictions on where calls can go to.
Social Media		Facebook, Twitter	PIO	PIO	Public access
GETS/WPS		All CMT members are issued GETS cards and have WPS on their court mobile phones	All CMT members	COOP Coordinator	GETS works on landline networks and can dial all numbers. WPS will give priority on mobile phones.
FirstNet Devices		One FirstNet phone located at each courthouse	Facility Manager	IT Director	No restrictions on where calls can go to. Phones can be used as mobile hotspots if needed.

Fax Lines		One fax located in the facilities department in every courthouse. Fax numbers stored on SharePoint site	All judges/staff	Facility Managers	Any available fax lines.
Building PA systems		Downtown and Juvenile courthouse have building wide PA systems	Facility Manager and Sheriff Staff. Messages sent from local control station.	Facility Manager	All building occupants in the Downtown and Juvenile courthouse.

Section 8 – Critical IT Vendors

When a cyber incident occurs, it is helpful to pre-identify IT vendors and the services they provide. Vendor services may be crucial to bringing operations safely back online, especially if staff availability is compromised or the scope of work created by an event is too large for internal staff to handle independently.

Vendor agreements often contain **service levels**, which indicate how quickly the vendor responds to and resolves issues. Some agreements, such as cyber insurance, are only engaged during an emergency.

The importance of vendor services should align with their relative involvement in returning essential functions and IT resources.

In the provided template, please identify your **top 5** critical IT vendors.

See Table 8 for a sample template of critical IT vendors.

See Appendix G for the blank template.

Table 8. Critical IT Vendors (Sample)

Name of Vendor	Provided Services	Point of Contact
CrowdStrike	Network and endpoint security	Todd Lopez
AT&T	Internet and firewall services	Tom Jones
Acme Insurance	Cybersecurity Insurance	Natalie Sims
Tyler Technologies	Case Management System (Family and Juvenile)	Victoria Do
Microsoft	Cyber incident response and consultation on existing cloud-based services	James Nguyen
Sheriff Cyber Crimes Division	County sheriff unit responsible for handling cyber-crimes within the county jurisdiction	Sgt. Allen Smith
AT&T	Cellular Service	Janice Williams

Section 9 – Endpoint Inventory

It is helpful to identify the endpoints the court maintains responsibility for to protect and restore its IT infrastructure. This will allow the courts to know where resources are located and how they may be reallocated if necessary to bring mission-essential functions back online. Conducting an inventory to determine what types of on-premises and virtual/cloud-based endpoints are in use and available are critical during a cyber incident. Since a cyber event may directly impact and compromise endpoints, having an inventory of these devices will assist with the impact evaluation, response, and recovery efforts.

Endpoints are network-connected devices such as PCs, Laptops, Printers, AV equipment, servers, network appliances, **etc., that are part of the court's overall infrastructure.**

Please identify **endpoints at the locations in this workbook and any critical endpoints needed for operations.**

See Table 9 for a sample table of an endpoint inventory.

See Appendix H for the blank template.

Table 9. Endpoint Inventory (Sample)

Endpoint Inventory – On-Premises

Type	Function	Location
Desktop computers	Workplace computing for staff and judicial officers	Courtroom (one at bench, one at chambers, one at clerk's desk), All non-management staff cubicles or offices.
Laptops	Workplace computing for management staff	All manager offices
iPads	Duty/night magistrate conducting emergency judicial matters (e.g., search warrants)	One iPad located at each courthouse.
Switches	Connectivity to court network	All IDF closets on 1st and 2nd floors of all courthouses
CCTV Servers	Servers which hold recordings for CCTV surveillance system.	1st Floor IDF Closet

Endpoint Inventory – Virtual/Hosted

Type	Name	Location
Email		
CMS	Case Management System	
Procurement Software	SAP	

Section 10 – Supporting Documentation

The following documentation (if available) should be collected and brought to the Cybersecurity and Disaster Recovery Workshop:

- Cyber incident response plan or similar related plans.

Section 10 - Supporting Documentation

- Infrastructure documentation and protocols to include but not limited to security appliances, monitoring solutions, and utilities (patch management, antivirus, malware, network, cloning).
- Data backup/recovery process and applicable testing standard operating procedures (SOPs).
- Policies that include but are not limited to cybersecurity, acceptable use, emergency procurement, communications, public records rules and disclosure, cyber insurance, and confidentiality.
- Organizational charts (e.g., court leadership, IT department, applicable contractors) or
- After action reports or any other incident reviews from actual cyber incidents or cybersecurity exercises.

****Secure Records Instruction**

For this workshop, please collect and retain the documentation securely. Securing the information may include using an encrypted device such as an encrypted flash drive or a secured connection to the cloud or other online storage. **Some of the information in the documentation listed may be sensitive or confidential. Please ensure this information is protected.**

Appendices

The blank templates (Appendix A-I) will also be delivered as a Word document (.docx).

Appendix A: Team Directories

As described in Section 1, please identify members of the court's Crisis Management Team (CMT) and IT Cyber Incident Response Team (CIRT).

Crisis Management Team (CMT) Directory

Name	Agency	Phone	Email

IT Cyber Incident Response Team (CIRT) Directory

Name	Agency	Phone	Email

Appendix B: Physical Locations

As described in Section 2, please identify all the physical locations your court system operates out of. If you are a statewide organization, please limit the locations to AOC and Supreme Court buildings.

Court Physical Locations

Name of Facility	Address

Appendix C: Business Impact Analysis of Essential Functions

As described in Section 3, please identify and document **5 (five)** essential functions for your court, the impact on your stakeholders if that function is not completed, and their respective Recovery Time Objectives.

EF Number	EF Description	Impact if EF is not completed	Recovery Time Objective
1			
2			
3			
4			
5			

Appendix D: Business Process Analysis of Essential Functions

As described in Section 4, please complete a BPA for each of the **5 (five)** essential functions identified in the previous section.

Each essential function has a dedicated table. Please ensure the appropriate table is completed.

Essential Function 1	Recovery Time Objective	Department Responsible	Key Staff
	Resources Needed		
	Work Location & Space Requirements		
	Supporting Activities		
	Internal Dependencies/Essential Records		
	External Dependencies/Essential Records		
	Manual Workarounds		
	Related Regulation		

	Can an Emergency Order provide relief?	☐ Yes ☐ No Notes:	
	Can EF be done via telework?	☐ Yes ☐ No Notes:	
Essential Function 2	**Recovery Time Objective**	**Department Responsible**	**Key Staff**
	Resources Needed		
	Work Location & Space Requirements		
	Supporting Activities		
	Internal Dependencies/Essential Records		
	External Dependencies/Essential Records		

Manual Workarounds	
Related Regulation	
Can an Emergency Order provide relief?	☐ Yes ☐ No Notes:
Can EF be done via telework?	☐ Yes ☐ No Notes:

Essential Function 3	Recovery Time Objective	Department Responsible	Key Staff
	Resources Needed		
	Work Location & Space Requirements		
	Supporting Activities		
	Internal Dependencies/Essential Records		

External Dependencies/Essential Records	
Manual Workarounds	
Related Regulation	
Can an Emergency Order provide relief?	☐ Yes ☐ No Notes:
Can EF be done via telework?	☐ Yes ☐ No Notes:

Essential Function 4	Recovery Time Objective	Department Responsible	Key Staff
	Resources Needed		
	Work Location & Space Requirements		

	Supporting Activities		
	Internal Dependencies/Essential Records		
	External Dependencies/Essential Records		
	Manual Workarounds		
	Related Regulation		
	Can an Emergency Order provide relief?	☐ Yes ☐ No Notes:	
	Can EF be done via telework?	☐ Yes ☐ No Notes:	
Essential Function 5	**Recovery Time Objective**	**Department Responsible**	**Key Staff**

Resources Needed
Work Location & Space Requirements
Supporting Activities
Internal Dependencies/Essential Records
External Dependencies/Essential Records
Manual Workarounds
Related Regulation

Can an Emergency Order provide relief?	☐ Yes ☐ No Notes:
Can EF be done via telework?	☐ Yes ☐ No Notes:

Appendix E: Technology Priorities

As described in Section 6, please identify **8 (eight)** critical IT applications and vital records. Once those are determined, prioritize the **top 5 (five)** for restoration during a cyber incident.

IT Application, Vital Record	Priority in Cyber Event	IT Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Unit Responsible, Point of Contact	Notes

Appendix F: Communication Modalities

As described in Section 7, please identify **all communication** modalities, and identify the **top 5 (five)** priorities.

Communication System	Priority in Cyber Event	Where is system located?	Who has access?	Unit responsible?	Who can receive communications?

Appendix G: Critical IT Vendors

As described in Section 8, please identify who your IT vendors are and what services they can provide. At a minimum, please list your top **5 (five)** critical IT vendors.

Name of Vendor	Provided Services	Point of Contact

Appendix H: Endpoint Inventory

As described in Section 9, please identify **endpoints at the locations in this workbook and any critical endpoints needed for operations.**

Endpoint Inventory – On-Premises

Type	Function	Location

Endpoint Inventory – Virtual/Hosted

Type	Name	Location

Appendix I: Supporting Documentation

The following documentation (if available) should be collected and brought to the cybersecurity summit:

- Cyber incident response plan or similar related plans.
- Infrastructure documentation and protocols to include but not limited to security appliances, monitoring solutions, and utilities (patch management, antivirus, malware, network, cloning).
- Data backup/recovery process and any applicable testing standard operating procedures (SOPs).

- Policies to include but not limited to cybersecurity, acceptable use, emergency procurement, communications, public records rules and disclosure, cyber insurance, and confidentiality.
- Organizational charts (e.g., court leadership, IT department, applicable contractors)
- After action reports or any other incident reviews from real cyber incidents or cybersecurity exercises.