

Dover, DE 2025 Cybersecurity Incident Response and Continuity of Operations Planning Annex

CONTINUITY

City of Dover, Delaware



PROJECT DETAILS

DIFFICULTY: High

COST: \$35,000

TIMEFRAME: 4 Months

DELIVERABLES: A comprehensive Cybersecurity IRP and COOP Annex specifically for the IT department.

CORE COMPETENCIES:

- Continuity of Operations Planning
- Cybersecurity Risk Management
- Disaster Preparedness
- Inter-Departmental Cooperation
- Stakeholder Engagement
- Federal Grant Compliance

PROJECT TEAM

Vision Planning and Consulting

CLIENT CONTACT

Kay Sass, Public Affairs and Emergency Management Coordinator
City of Dover
PO Box 475
Dover, DE 19903
Phone: (302) 736-7003
Email: ksass@dover.de.us

PROJECT OVERVIEW

Following a series of cybersecurity breaches and attacks affecting the City of Dover, Kent County, and the State of Delaware, the City engaged VPC to develop its first-ever Cybersecurity Incident Response Plan (IRP). The initiative aimed to formalize cybersecurity protocols, strengthen the IT Department's defensive posture, and align municipal operations with recognized best practices.

PROJECT SUMMARY

Through extensive information gathering and stakeholder collaboration, VPC documented Dover's existing capabilities across hardware inventory, virtualization platforms, backup infrastructure, and vendor relationships. We created customized worksheets that converted ad hoc practices into structured, auditable processes—laying the foundation for a repeatable and measurable cybersecurity program.

The IRP was built around the six (6) core functions of the NIST Cybersecurity Framework 2.0—Govern, Identify, Protect, Detect, Respond, and Recover. It established clear incident-classification procedures, defined response roles, and designed escalation matrices tailored to municipal operations. VPC embedded detailed compliance crosswalks throughout the document, directly mapping each section to State and Local Cybersecurity Grant Program (SLCGP) Elements 1, 4, 5, 7, and 11, streamlining future audit and grant-review processes.

Recognizing the risk cyber incidents pose to essential city services, VPC also developed a specialized Continuity of Operations Plan (COOP) Annex. This annex identified critical IT functions, succession protocols, and alternative facility operations, while incorporating Recovery Time Objectives (RTOs) for Dover's most vital systems—emergency dispatch, utility SCADA,

and financial platforms—to ensure prioritized restoration during incidents.

To support long-term resilience, VPC created an innovative three-year cybersecurity funding roadmap through 2027, outlining key initiatives such as SIEM expansion, multi-factor authentication deployment, and encrypted backup replication. This roadmap positions Dover to strategically leverage federal grant opportunities, thereby strengthening its cybersecurity infrastructure. Deliverables included Appendices for SLCGP 2024 NOFO-compliant Project Worksheets, ransomware preparedness matrices, and crisis communication templates for seamless integration with state and regional cybersecurity networks.

Despite challenges—such as extended grant disbursement delays and IT staff turnover during critical development phases—VPC applied adaptive project management and flexible engagement strategies to maintain momentum. By leveraging established relationships and providing ongoing support to new team members, VPC ensured continuity and on-time delivery. The final deliverables package transformed Dover from informal cybersecurity practices into a compliance-ready, grant-eligible organization with documented, tested procedures for incident response and continuity of operations.