CITY OF BANNING
STAFF REPORT

TO:	**CITY COUNCIL**
FROM:	**Arturo Vela, Acting City Manager**
PREPARED BY:	**Barbara Mason, Chief Procurement Officer** **Michelle Green, ASD**
MEETING DATE:	**August 26, 2025**
SUBJECT:	**Consideration of Resolution 2025-117 Approving the Budget Allocation to Renew Agreement with Vigilant for Cybersecurity Monitoring, Threat detection, & remediation**

RECOMMENDATION:

Adopt Resolution 2025-117

BACKGROUND:

In today's digital landscape, cybersecurity has become a critical priority for organizations. With the increasing reliance on online platforms to store sensitive customer data, financial records, and the City's intellectual property, businesses are increasingly vulnerable to sophisticated cyber threats. The protection of digital assets is no longer optional-it is essential. Traditional, off-the-shelf solutions such as antivirus software and firewalls are no longer sufficient on their own. Cybercriminals continue to evolve, employing advanced tactics that can bypass conventional defenses. To effectively safeguard the City's computing environment, a comprehensive and proactive cybersecurity strategy is required—one that addresses all facets of security, including people, processes, and technology. Implementing robust monitoring and response service is vital. Such a service enhances the City's ability to detect and respond to anomalous activity in real time, enabling swift action to mitigate threats. This not only reduces potential financial and reputational damage but also strengthens the overall resilience of City operations against cyberattacks

JUSTIFICATION:

Cybersecurity is essential to ensuring the confidentiality, integrity, and availability of the City's information systems. These systems encompass a wide range of sensitive assets, including personally identifiable information (PII), personal data, intellectual property, and critical governmental and industry-specific information. Without a comprehensive cybersecurity program, the City remains highly vulnerable to data breach campaigns, making it an attractive target for cybercriminals.

A robust cybersecurity monitoring and response framework offers numerous strategic benefits, including:

- Minimizing the risk of data breaches
- Enhancing response times to cyber incidents

- Safeguarding personal and sensitive data
- Identifying and addressing security vulnerabilities
- Ensuring compliance with regulatory standards
- Reducing operational downtime
- Preserving public trust and organizational reputation
- Improving data governance and management
- Strengthening the City's overall cybersecurity posture

Investing in proactive cybersecurity measures is not only a technical necessity, but also a foundational component of responsible governance and operational resilience.

FISCAL IMPACT:

Total Cost per renewal year 2026-2027 $103,303.

ALTERNATIVES:

1. Approve as recommended
2. Do not approve and provide alternative direction

BUDGETED?:

Yes

CONTRACT/AGREEMENT:

Yes

ATTACHMENTS:

1. Attachment_1-_Resolution_2025-117_Agreement_with_Vigilant_Managed_Endpoint_Detection_and_Response__MEDR_.docx
2. Presentation.pptx
3. City of Banning_Vigilant 1 Year Renewal Agreement 7.9.2025.pdf