



GOV. CHRIS CHRISTIE | LT. GOV. KIM GUADAGNO | DIR. CHRIS RODRIGUEZ

NJOHSP

OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

County Cyber Grant Funded Projects

Project

Purchase an Intrusion Detection and Prevention System (IDS/IPS) appliance that integrates with the existing county network.

Justification

With the rapid emergence of internal threats, and those that easily bypass traditional perimeter security defenses, the counties must think about security beyond the perimeter. To assist the counties with a layered security deployment strategy, grant funding has been made available for the purchase and integration of an IDS/IPS appliance to be placed into the county network. The placement of the appliance is at the discretion of the county information technology director.

Expectations of the County

The IDS/IPS appliance must be integrated into the county network. Mitigation and remediation of identified cyber threats are the responsibility of the county.

Reporting

To ensure statewide cyber situational awareness, identified cyber threats meeting severity level 2/3/4/5 must be reported to the OHSP's Counter Terrorism (CT) Watch where it will be entered as a cyber Suspicious Activity Report (SAR). Distribution of the cyber incident SAR will be to the cyber incident notification group managed by OHSP and the N.J. Office Information Technology (OIT). This condition is being applied to support and facilitate the build out of a statewide cyber security information sharing capabilities.

If applicable, the NJ Cyber Fusion Cell will notify the Multi-State Information Sharing and Analysis Center (MS-ISAC) of the incident. MS-ISAC will coordinate with the federal government and provide assistance with remediation strategies if requested by the State of New Jersey.

Severity Level 2:

This severity level indicates a change in normal activity with minor level impact; a vulnerability is being exploited with minor impact; infected by malware with the potential to spread quickly; compromise of non-critical system(s) that did not result in loss of sensitive data; and/or a distributed denial of service attack with minor impact.

Severity Level 3:

This severity level indicates a significant risk due to an exploit for a vulnerability that has a moderate level of damage or disruption; compromise of secure or critical system(s); compromise of system(s) containing sensitive information or non-information; more than one entity (agency)

Attachment M



GOV. CHRIS CHRISTIE | LT. GOV. KIM GUADAGNO | DIR. CHRIS RODRIGUEZ

NJOHSP

OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

affected in the network with a moderate level of impact; infected by malware that is spreading quickly throughout the internet with moderate impact; and/or a distributed denial of service attack with moderate impact.

Severity Level 4:

This severity level indicates a high risk of malicious activity impacting core infrastructure; a vulnerability is being exploited and there has been major impact; data exposed with major impact; multiple system compromises or compromises of critical infrastructure; attackers have gained administrative privileges on compromised systems; multiple damaging or disruptive malware infections; mission critical application failures but no imminent impact on the health, safety or economic security of the State; and/or a distributed denial of service attack with major impact.

Severity Level 5:

This severity level indicates a severe risk due to malicious activity resulting in widespread outages and/or complete network failures; data exposure with severe impact; significantly destructive compromises to systems, or disruptive activity with no known remedy; mission-critical application failures with imminent impact on the health, safety or economic security of the State; compromise or loss of administrative controls of critical systems; and/or loss of critical supervisory control and data acquisition (SCADA) systems.

Managed/Monitored Services

With an endless emergence of new threats and county resources under constant pressure, it can be difficult to balance all of the strategic and operational tasks required for an effective information security program. IDS/IPS appliances can provide a highly effective layer of security designed to protect critical assets from cyber threats. Organizations can detect attempts by attackers to compromise systems, applications and data by deploying network IDS; however, keeping the devices tuned and up-to-date so they are effective is a challenge for many organizations.

Managing/Monitoring IDS/IPS devices requires a specialized skill set, because the devices are only effective if they are well tuned to the current threats and the network in which they are deployed. IDS devices can generate thousands of alerts each day and are very prone to false positives, making it difficult to identify true threats and take timely action to protect assets. Acquiring a managed/monitored service can help alleviate this burden and enable more effective operation of your intrusion detection and prevention technologies.

Attachment M
