To: **Bay Area UASI Approval Authority**

From: **Mike Sena, Executive Director NCRIC**

Date: **June 10, 2021**

Re: **Item 10: NCRIC Cyber Threat and Critical Infrastructure Protection Briefing**

Recommendations:

No recommendation

Action or Discussion Items:

Discussion

Discussion/Description:

NCRIC Executive Director Mike Sena will present a threat briefing on Cyber Threats and Critical Infrastructure Protection.

In the first half of 2021, nationwide Microsoft Exchange Server and Pulse Secure VPN vulnerabilities turned everyday IT technicians into cyber threat hunters. Existing NCRIC connectivity with law enforcement and municipal and county government IT practitioners allows efficient identification of new victims in such large scale incidents. NCRIC consistently works with these partners through Biweekly Cyber Threat calls and the UASI/NCRIC Cyber Resilience Workgroup to maintain awareness, offer mitigation options and coordinate access to remediation resources in the event of a cyber incident.

In addition to supporting local victims in remediating large scale incidents, the NCRIC Cyber Security Team handled 54 Cyber Suspicious Activity Reports (Cyber SARs) in the first half of 2021. Incident types show ransomware, business email account compromise, and denial of service conditions most impacted victim organizations in the NCRIC Area of Responsibility (AOR). Email-based attacked remained the most common infection vector, with social engineering tactics targeting executives and multiple victims across critical infrastructure sectors. This briefing will highlight how ransomware infections have become synonymous with data breaches, local critical infrastructure incidents tied to national cyber threats, the consequences of a lapse in vendor supply chain security, and measures for mitigating denial of service conditions against communications assets.