DAVID Y. IGE
GOVERNOR

TODD NACAPUY
CHIEF INFORMATION
OFFICER

STATE OF HAWAI'I
OFFICE OF INFORMATION MANAGEMENT AND TECHNOLOGY
P.O. BOX 119, HONOLULU, HAWAI'I 96810-0119
www.hawaii.gov/oimt

OIMT-CORR 15.0113

MEMORANDUM

September 1, 2015

TO: CIO Council Members

FROM: Todd Nacapuy, Chief Information Officer

SUBJECT: Use of Desktop Sharing Software on the State Enterprise Network

A potential vulnerability has been identified on the State Network due to the use of TeamViewer and Windows Remote Desktop Connection (RDC), commercial software used for remote maintenance and support and other remote access/control.

Effective September 3, 2015, general use of TeamViewer and RDC with parties outside the State Network will be blocked (internal use will be allowed). If external use is needed, it will require the approval of the State Security Operations Center (SOC).

For departments' reference, the SOC will post to the CIO Council secure site a spreadsheet identifying, by department, IP addresses suspected of using TeamViewer or RDC.

Requesting Use of TeamViewer/RDC

All departmental DP Coordinators requesting use of TeamViewer and/or RDC on the State Network are responsible for emailing the following information to the SOC at soc@hawaii.gov as well as promptly notifying the SOC when this information changes:

1. Computer name and IP addresses (or Dynamic Host Configuration Protocol / DHCP scope) requiring the software

2. Specification of whether the software is required for collaboration or remote maintenance

3. Justification for use

4. Has a license been purchased? If so, what kind of license?

Note: For TeamViewer only, if use is granted, configuration must adhere to the guidelines provided on the following page.

TeamViewer Configuration (if use is granted)

Description	Department Responsibility
If user requires TeamViewer for collaboration only	Disable remote maintenance
If user requires TeamViewer for remote maintenance	• Ensure TeamViewer is installed as an application (not as a service) • Configure TeamViewer to not allow "unattended access" • When remote access is needed, set a one-time password and provide it to the user securely; change password and disable once session is over • If using static addresses, user must provide source IP address and computer name to the SOC; otherwise, user must provide DHCP scope
If user does not require TeamViewer	**Uninstall TeamViewer immediately**

Desktop sharing software introduce vulnerabilities into the State system. Many data breaches involve remote access services, as attackers can exploit it.

While this memo is specifically about TeamViewer and RDC, departments should review all other software allowing remote connections and take steps necessary to limit the risk to the internal network. If the connections are no longer needed, the software should also be uninstalled or disabled. If the connections are still needed, steps should be taken to mitigate the risk of the connection being used to compromise the network. The SOC can provide additional guidance and help if needed.

Compliance is mandatory in order to ensure the security on the State Network.

c: Security Operations Center
DP Coordinators