Information Privacy and Security Council

PERMITTED INTERACTION GROUP
Report and Recommendations
Submitted April 19, 2017

TO: Information Privacy and Security Council

FROM: Permitted Interaction Group

SUBJECT: Handling of Personally Identifiable Information on Mobile Devices

This report conveys to the full Information Privacy and Security Council (IPSC) the recommendations of the Permitted Interaction Group (the Group) assigned to make recommendations on the handling of personally identifiable information (PII) on mobile devices.

INTRODUCTION

In its monthly meeting on December 21, 2016, the IPSC voted to form a Permitted Interaction Group on the handling PII on mobile devices. Members of the Group are IPSC Members/Designees Vincent Hoang, David Keane, Lim Yong and Wilfredo Tungol, as well as IT Governance Officer Todd Omura and Senior Communications Manager Keith DeMello of the Office of Enterprise Technology Services (ETS).

The Group convened on two occasions: February 6 and March 22, 2017.

BACKGROUND

Throughout 2016 and early 2017, the IPSC discussed policies, standards and procedures relating to the handling of PII, consistent with its roles and responsibilities outlined under Hawai‘i Revised Statutes (HRS) sections 487N-5 and 487N-6. This included amendments to procedures for internal processes with regard to handling PII in hard-copy form, which were communicated to the Department of Human Resources Development on February 21, 2017, for appropriate action.

A secondary outcome of the IPSC's discussions was agreement that the IPSC should address the "technology" piece of handling of PII — on mobile devices and *personal* mobile devices in particular. Devices vary widely, and department-level policies, device management processes, and employee education employee about risks and best practices are all at various stages, and at least one county is close to selecting a mobile device management solution.

DISCUSSION

For the purposes of this report, mobile device refers to all devices and accompanying/related media that fit the following classifications:

- mobile/cellular telephones;
- smartphones and tablets w/mobile operating system (OS);

- other mobile OS, PC/laptop or removable storage devices capable of storing email and/or data that can connect or store State data; and
- any hardware and related software that could be used to access State resources, particularly if the equipment is NOT State-approved, -owned or -supplied.

Existing resources were discussed, including the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce, a recognized authority on technology standards across public and private sectors. NIST Special Publication 800-124, Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," provides relatively current guidelines to help organizations centrally manage and secure mobile devices against a variety of threats. It further provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use, including securing both organization-provided and BYOD mobile devices.

It was also acknowledged that a draft Mobile Use Policy developed by the State of Hawai'i Enterprise Architecture Working Group is still under review by ETS and relevant agencies. The goal of the policy is to "protect the integrity of the private and confidential data that resides within the State's technology infrastructure." The policy is intended to prevent data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network, where it can potentially be accessed by unauthorized resources and/or persons. As the draft policy states, a breach of this type could result in:

- loss of information and revenue;
- damage to the integrity of data, applications, and the State's public image; and
- liability to the State or its citizens.

It is anticipated that the draft Mobile Use Policy will address many of the same issues being discussed by this Group, as it would apply to all employees of the State of Hawai'i and any persons under consulting contract, independent contractor agreement or otherwise hired that connect to any physical, logical, and/or electronic premise of the State to access, process, store, and/or transmit State data using a mobile device. **Once approved, the intention is that the Mobile Use Policy would allow each State entity to have supplemental policies on mobile device usage that may change or enhance the baseline policy, based on business need and/or unique risk held by that State entity.**

During the Group's discussion, it was agreed that clear distinction should be made between State-issued mobile devices and personal mobile devices (e.g., Bring Your Own Device / BYOD). It was the general feeling of the Group to allow State-used mobile devices but recommend against BYOD, unless specific rules and specifications are followed and agencies understand that they are assuming the risk on their own.

RECOMMENDATIONS

The following are the Group's recommendations to the IPSC:

1. **Identify NIST Special Publication 800-124, Revision 1, as a guideline for local and State agencies**

In accordance with its statutorily mandated duties under HRS section 478N-6, the IPSC is responsible for identifying best practices to assist government agencies in improving security and privacy programs relating to personal information. As NIST Special Publication 800-124, Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," provides current guidelines on this matter, it is prudent for the IPSC to formally identifying the publication (and subsequent revisions pending future review) as providing credible guidance on this matter for local and State agencies within Hawai'i.

2. Advise agencies to allow personal mobile devices ONLY IF specific requirements are met

In recognition of security concerns and the high standard applicable to government agencies in safeguarding the public's data, the IPSC should clearly specify the conditions under which personal mobile devices may be employed for county and/or State business. This additional guidance would specify that personal mobile devices may be used provided that the following requirements are met:

- Device is approved by the agency's lead IT official;
- User agrees to follow guidelines provided by NIST Special Publication 800-124, Revision 1;
- User affirms that standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other Federal and State laws are met, if applicable to the information being handled by the user and/or the agency;
- User agrees to any additional use parameters specified by the agency; and
- User acknowledges that the device and the entirety of its contents may be subject to eDiscovery, as allowable by law.

3. Communication of Guidance

Timely communication and awareness are of critical importance to information privacy and security. It is recommended that the IPSC conduct the following communications activities once formal action is taken regarding the above:

- provide communication of action via memorandum to all agency privacy designee statewide;
- post the name of the publication, a brief description, and hyperlink to the online publication (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) to the "Guidelines & Best Practices" section of the IPSC's website (ipsc.hawaii.gov); and
- consider transmitting tips and resources to the network of agency privacy designees via regular (e.g., monthly) email notices to reinforce guidance.