DRAFT REPORT

Report [_____] of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection the Department's transition to cloud services technologies and enhanced capabilities

As approved in Public Session

on [_____]

Background

On October 27th, 2020, former Chief Privacy Officer Dena Kozanas tasked the Data Privacy and Integrity Advisory Committee (DPIAC) to:

> Consider the Department of Homeland Security's (DHS) transition to cloud service technologies and the enhanced capabilities this transition has provided the Department during the COVID-19 telework environment to determine if there are associated privacy risks that would merit a near-term tasking.

Given this tasking, the Emerging Technologies Subcommittee (the ET Subcommittee) held meetings internally and with representatives of the Office of the Chief Information Officer (OCIO) to better understand the transition the Department has undergone due to the COVID-19 outbreak. Additionally, the ET Subcommittee has conducted interviews, reviewed documents provided by the OCIO, and assessed the policies and precautions currently being taken around access to data, data integrity during migrations, classification of personally identifiable information (PII), and additional potential privacy concerns.

DHS Cloud Migration Overview

During the October 27, 2020 DPIAC meeting, then Chief Information Officer Karen S. Evans briefed the DPIAC on the transition her office facilitated to enable teleworking and additional cloud migrations during the COVID-19 pandemic. Supporting this shift was no small task for DHS where an average daily load of 10,000 teleworkers suddenly turned into 70,000 as offices throughout the country were closed for in-person work. In addition to the 7x number of teleworkers, the Homeland Security Information Network (HSIN) saw a 200% increase in traffic and the DHS HQ Virtual Private Network (VPN) increased in usage by 483%.

For any organization, this type of shift would be overwhelming at best, however DHS was able to make the shift without a disruption in operations. DHS was able to meet this increased demand in part due to its experience in the winter of 2018/2019 when snowstorms forced a large number of DHS employees into teleworking. That experience

in 2018-19 prompted more wide-spread use of DHS' VPN and helped drive the push for continued migration to cloud-based collaboration and productivity tools using the Microsoft Office 365 suite of tools.

Outside of the cloud productivity tools and teleworking, DHS has an ongoing migration and modernization of data and services that it supports. DHS is able to improve service availability, reliability, and cost effectiveness through a three-pronged approach, including:

- Migration of data, services, and computing to the cloud, where possible.
- Consolidation of datacenter operations
- Modernization of remaining systems

In talking with officials from the OCIO, they reported all systems which have not yet been moved to the cloud are accounted for and identified. Each system has undergone evaluation to see if it can be moved into the cloud; for those that the OCIO determines are not able/ready to move into the cloud, justification for it staying in on-premises datacenters is documented. Additionally, these legacy systems are currently being rebuilt with modern technology to ensure they continue to perform and provide the same level of resilience and security as their cloud counterparts.

Risks of Cloud Migration

While the benefits of modernization and migration to the cloud, where applicable, are many, it does not come without risks to security, privacy and data integrity. These risks often do not outweigh the benefits, but nonetheless should be taken into account as the decision to migrate systems and data to the cloud are taken.

Data security in cloud migrations is not just about physical security of the servers, it also relates to the ability to keep sensitive data private. Prior to migrating the data, the primary consideration should be an inventory of the data to be migrated, and what access and sharing permissions exist in current systems. Then throughout the migration these access and sharing permissions need to be maintained to prevent data leaking into insecure systems. When the data is finally in the final cloud location, these controls need to be finalized to help prevent future data leaks.

Data integrity is a second consideration which can often be overlooked or understated as a concern in migrations. It is critical to ensure process is followed for how data is modified, by whom, and eventually how it is archived. Data in motion, as it is during a migration, has risks associated not only with malicious alterations en-route, but also data loss from incomplete transfers and additional non-secured copies and backups

made during the process going unaccounted for. Proper planning, and audits once finished, allow for the data integrity to be maintained. Also important during the migration planning and process is planning for data retention. Cloud systems can simplify data backup and redundancy but inherit with this is the risk that data remains beyond the time necessary and thus providing a risk for security and privacy. For this reason, migrations should also include long term planning for where data will be stored, how many copies created for redundancy, and proper deletion of data once it is past the point of usefulness.

Third in consideration during data migrations is privacy. While data may be kept private in on-premises systems out of the nature of its location, moving data to the cloud can have an effect on data not previously classified as Personally Identifiable Information (PII) to find ways into data sets which are now inherently more accessible. For this reason, proper identification of the data being migrated, even if it has already been audited, any PII it may contain. During this process, it is also a good step to review the methods to determine what is considered PII, who is responsible for making the designations, and what if any processes need to be updated once data is marked as PII to keep it secure. This ensures as the systems are updated, the responsibility matrix for the data stays up to date as well.

Findings

After reviewing provided documents, meeting with the OCIO, and evaluating the information shared with us, the ETy Subcommittee finds that DHS' ongoing cloud migrations have been conducted with appropriate care and effort to keep data secure, private, and available. This occurring against the backdrop of a global pandemic and unprecedented shift to remote work by DHS is to be commended.

It appears to the ET Subcommittee that existing policies and management directives are being followed as expected. To ensure DHS policies are followed, audits occur prior to, during, and after implementation and migration. The frequency of the recurring audits by OIG and how systems are selected is a potential new tasking the DPIAC, or this subcommittee, can look into further.

In situations where Management Directives don't yet exist, DHS is working directly with the software providers to follow industry practices and standards, while simultaneously updating and implementing appropriate Management Directives. This is a reasonable approach as technology improvements can occur faster than policy changes. Working with their technology partners and providers, while simultaneously updating and implementing appropriate Management Directives, helps to cover for the gaps in policies while they are updated and written.

Recommended Next Steps

Based on our review and the findings above, the ET Subcommittee recommends three areas of further study and action:

As Management Directives play a critical role in providing guidance to DHS, our first recommendation is that DHS conduct a review and inventory of the Management Directives and addendums currently in place to ensure any new cloud technologies used during this migration are appropriately covered by internal policies. While relying on technology partners and providers to implement best practices is a good and helpful safeguard, it is in the best interest of DHS to continue to both create new Management Directives, and update existing policies, with regard to new technologies and techniques. This helps to ensure consistency across DHS via a shared oversight of technology (rather than relying on the cooperation of partnerships with technology providers).

Secondly, we recommend that DHS review its OIG audit process to ensure that after an initial cloud migration, ongoing audits are conducted in an appropriate cadence to ensure that as systems and data continue to change, the audits can provide ample coverage and promptly identify issues which may arise after the initial migration.

Lastly, we recommend that DHS proactively include and evaluate both a privacy and security review early on in any discussion of system, tool, or data migration, to help manage risk and “bake” proper privacy and security safeguards into the planning and execution from the beginning. By including the technology and policy groups in early discussions, Privacy by Design principles can become the default by which systems are created and data migrated, instead of being ‘caught’ in a later audit stage.