Physical Security Evaluation of
Department of Social Welfare and Development (DSWD) ICT Infrastructure

This evaluation focuses on the physical security of the ICT infrastructure of the Department of Social Welfare and Development (DSWD), specifically examining the Field Office 12 Data Center (FO12.ENTDSWD) and its related components.

1. Data Center Security (FO12.ENTDSWD)

Strengths:

- Positioned within the ICTMS, the data center benefits from the broader organizational security structure.
- A strict policy limits physical access to authorized personnel only, reducing the risk of unauthorized entry.
- Equipped with a heavy-duty UPS, automatic transfer switches, and an industrial-grade generator to ensure operations remain uninterrupted during power outages.
- Air conditioning and overheating monitoring systems are in place to maintain optimal environmental conditions for equipment.
- Surveillance cameras, biometric access controls, intrusion detection systems (IDS), and a dedicated monitoring team are implemented to address and respond to physical security threats.

Areas for Improvement:

- Limiting access to one authorized individual reduces the attack surface but creates a single point of failure. Implementing a backup personnel policy or multi-person authentication is advisable.

2. Internal Infrastructure Security

Strengths:

- The use of Intermediate Distribution Frames (IDFs) connected to a Main Distribution Frame (MDF) enables efficient network segmentation and control.
- Palo Alto Next-Generation Firewalls (NGFW), routers, and intrusion detection systems offer high-level threat prevention and response.
- Use of Cat6e cables and organized patch panels supports better network performance and simplifies maintenance.

Areas for Improvement:

- The IDF and MDF systems have been operational for over 10 years, with regular preventive and protective maintenance. However, key components have not been replaced during this period, making them increasingly susceptible to wear and tear.

3. Device and Data Security

Strengths:

- Devices are registered under an Active Directory domain, allowing synchronized user profiles and remote software deployment.
- Cortex XDR is deployed across devices to ensure real-time threat detection and response.
- Policies are enforced to prevent unauthorized software installations, with attempts logged for review.
- GlobalProtect VPN provides encrypted and authenticated access for users operating outside of office premises.

Areas for Improvement:

- Laptops and tablets used in the field are not equipped with full-disk encryption. If lost or stolen, these devices may lead to data breaches. Encryption should be implemented to protect sensitive information.

4. Backup and Disaster Recovery

Strengths:

- A mix of full and differential backups ensures reliable data restoration.
- Backup data is stored on a dedicated NAS within the premises.
- NAS backups are mirrored to a secure offsite location in General Santos City, supporting disaster recovery efforts.

Areas for Improvement:

- To further enhance flexibility and ensure data availability during large-scale disruptions, it is recommended to incorporate a cloud-based backup solution like Amazon Web Services (AWS) database backup services.