MEMORANDUM

Date: August 13, 2021

To: All Agency Information Technology Leadership

From: Charles "Chip" Stewart IV, State Chief Information Security Officer

Subject: **Teleworking Printer Guidance**

The shift to remote work that occurred in 2020 required significant flexibility from both employees and agencies. Recently, agencies have requested guidance from DoIT regarding employee use of personally owned printers at the employee's residence, printing services, and advice on related security implications. Therefore, the Office of Security Management offers the following **guidance** regarding this matter:

- The use of cloud printing services is prohibited, unless such use is covered under an existing contractual relationship between the State of Maryland and the service provider.
- Units should prohibit employees from using personal printers to print documents containing:
    - Personal Information/Personally Identifiable Information, as defined in MD State Gov't Code §10-1301
        - However, a user may use a personal printer to print their own personal information or that of a family member.
    - Information covered by certain regulations, such as:
        - Federal Tax Information;
        - Protected Health Information; and
        - Payment Card Industry Data (credit card information).

Regardless of where documents are sourced, the obligation to protect sensitive information remains. Any printed documents containing sensitive information should be properly secured when not in use and destroyed in accordance with applicable policies and guidelines.

While this memo should not be construed as a statement of policy, it does intend to provide clarity on DoIT's position regarding the use of personal printers and printing services while teleworking. Ultimately, the risk-management decision falls to the unit's executive leadership.

Please feel free to email questions to doit.intake@maryland.gov.

Sincerely,

Charles "Chip" Stewart IV
State Chief Information Security Officer