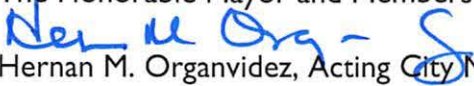




CITY OF DORAL Office of the City Manager Letter to Council

LTC No. 013-2022

To: The Honorable Mayor and Members of the City Council
From: 
Hernan M. Organvidez, Acting City Manager
Date: April 11, 2022
Subject: **Nationwide Cybersecurity Review**

The United States Congress directed the U.S. Department of Homeland Security (DHS) to develop a cyber-network security assessment that would measure gaps and capabilities of state, local, tribal, and territorial (SLTT) governments' cybersecurity programs. The Nationwide Cybersecurity Review (NCSR) assessment is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by the Department of Homeland Security (DHS) & the Multi-State Information Sharing and Analysis Center® (MS-ISAC®).

The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial (SLTT) governments. FEMA has made the NCSR a requirement for recipients and sub-recipients of the two major programs under the Homeland Security Grant Program (HSGP), the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI). In addition, this is required if we want to get any type of federal grants for security projects.

The NCSR is scored on a seven-point scale, with (7) seven being the highest possible score and (1) one being the lowest. The minimum recommended maturity level for SLTT governments is a score of five (5) on the NCSR scale. Below please find Figure one that illustrate NCSR Maturity.

FIGURE 1

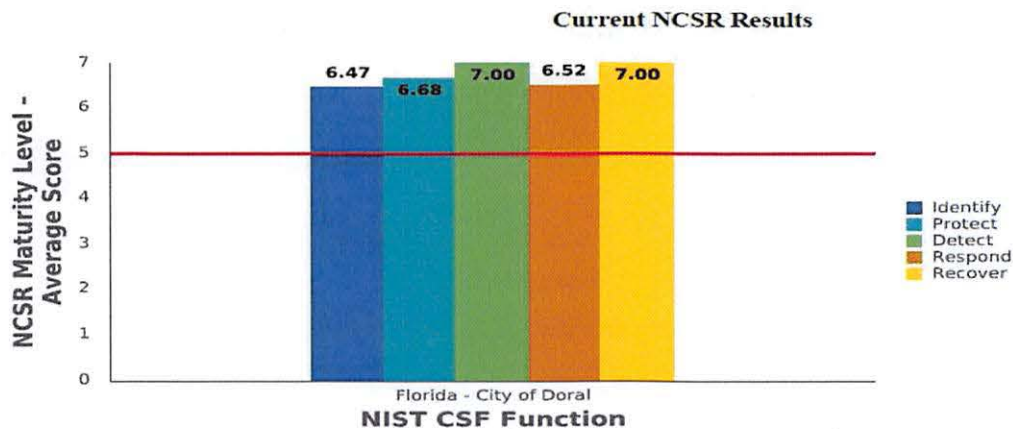
Figure 1 provides a full breakdown of the NCSR Maturity Level response scale along with the scores associated with each maturity level.



The assessment Framework Core elements work together as follows:

- Identify – Organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect – Implement appropriate safeguards to ensure delivery of critical services.
- Detect – Implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover – Implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Below are the results of the City of Doral NCST assessment results in which our cybersecurity maturity level is much higher than the minimum. This indicates the City of Doral Information Technology department has been focused on policy and procedure development to formalize cybersecurity activity including actively monitoring for cybersecurity events and remaining vigilant to threats.



The red line indicates an average score of 5, which is designated as the recommended minimum maturity level

The Information Technology Department continues to focus on improving and guarantee resilience, security, quality assurance and high availability of services during emergency events as well as during normal operations. The Mayor and Council office continued support helps us work towards our mission of improving the City's overall cybersecurity posture.

c. Gladys Gonzalez