



John A. Carey
Inspector General

OFFICE OF INSPECTOR GENERAL PALM BEACH COUNTY

TIPS AND TRENDS #2020-0006
JUNE 2020



Inspector General
Accredited

Tips and Warnings from the Palm Beach County Office of Inspector General and Other Offices of Inspectors General Related to COVID-19

Risks While Government Employees Work Remotely

Due to the COVID-19 pandemic, many government entities are allowing employees to work remotely. Remote work presents many challenges, and in government it presents unique circumstances and risks.

Advantages of working remotely include:

- Addresses current health concerns
- Employee flexibility during pandemic-related restrictions
- Saves employee commuting costs and time
- May improve worker productivity and employee morale

Pitfalls that exist when working remotely include:

- Cyber security risks
- Confidentiality and public disclosure issues
- May decrease worker productivity and increase employee stress



Cyber Security

As government employees work remotely, cyber security risks may rise. Agencies should ensure the security of their work products and systems by using virtual private networks (VPNs) and agency-certified cloud based networks with strong passwords and/or two-factor authentication protocols. Failure to do so may put sensitive government data at risk. Government supervisors and information technology professionals should regularly confirm that these safeguards are in place.

Confidentiality and Public Disclosure

Employers should ensure their employees are familiar with and continue to comply with any agency confidentiality policies and are cognizant of their continued duty not to share restricted government information or records with family and friends in their remote work locale. In addition, government employees and officials should remain cognizant of their duties and responsibilities regarding records retention and access to public records in

“Enhancing Public Trust in Government”

accordance with Chapter 119, Florida Statutes, and their duties and responsibilities relating to public meetings as set forth in Chapter 286, Florida Statutes.¹

Tips and Warnings from Federal Offices of Inspectors General Related to COVID-19 Scams

Be Alert for Scammers

Working remotely may increase employees' exposure to scammers through personal or work emails, phone calls, texts, social media, or in-person. Scams and fraud activity is particularly high during public emergencies as scammers take advantage of people's confusion and fear to lure them into disclosing bank accounts, social security numbers, medical information, and other sensitive information. If your personal information is stolen or shared with scammers, it may be used in other schemes.



Below are selections of tips and warnings from Federal Inspectors General:

U.S. Department of Health and Human Services Office of Inspector General

- Be cautious of anyone asking for your Medicaid number or other health insurance information.
- Be suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies.
- Ignore offers or advertisements for COVID-19 testing or treatments on social media.
- A doctor or other trusted healthcare provider should assess your condition and approve any requests for COVID-19 tests.

U.S. Department of Housing and Urban Development Office of Inspector General

- Housing and Urban Development (HUD) does not initiate contact with individuals regarding its assistance or about obtaining assistance. If somebody contacts you without you contacting them first and claims to be from HUD or offering HUD assistance, be suspicious. Obtain the person's contact information and call HUD directly to verify whether they are legitimate, or just hang up or delete the email.
- If you are contacted by an unfamiliar organization claiming to be a nonprofit or one that has a name very similar to that of a well-known nonprofit, be suspicious. Someone may be falsely claiming to be helping victims of COVID-19. Provide charitable donations directly to organizations you know, or visit the Internal Revenue Service (IRS) site at <https://www.irs.gov/charities-and-nonprofits> to verify that a nonprofit is registered with the IRS.
- If you receive a call or email from someone stating they are from a reputable company or a company you may already be doing business with asking for

¹ Consult your agency attorney regarding the impact of any Temporary Emergency Orders relating to public meetings.

passwords or bank or credit card information, be suspicious. You may see a link that looks official but is not. Often, a scammer will make the need for information seem urgent to get you to respond. Go directly to websites or call businesses directly - legitimate requests usually will not require you to provide personal information.

U.S. Department of Treasury Office of Inspector General

- Government entities will rarely contact you by any means other than U.S. Mail, including by text, call, or email, regarding federal programs. Up to date information is available about individual economic impact payments under the CARES Act at www.irs.gov/newsroom/economic-impact-payments-what-you-need-to-know. Currently, this is the only federal program for direct grants, reimbursements, or other types of individual financial payments.
- If you receive calls, emails, or other communications claiming to be from the Treasury Department and offering COVID-19 related grants or stimulus payments in exchange for personal financial information, an advance fee, or a charge of any kind, do not respond. These are scams.

Resources are Available to Identify and Report Fraud, Including:

- U.S. Department of Justice at www.justice.gov/fraudtaskforce/report-fraud/chart
- Federal Bureau of Investigation at www.ic3.gov
- National Center for Disaster Fraud Hotline (866)720-5721 or www.disaster@leo.gov
- U.S. Department of Homeland Security at www.COVID19Fraud@DHS.gov

You can also report suspected fraud, waste, abuse, or mismanagement to your Palm Beach County Office of Inspector General:

THE MANY WAYS TO REPORT FRAUD TO THE OFFICE OF INSPECTOR GENERAL



REPORT FRAUD CONFIDENTIALLY BY CALLING FIRST