TEAM YOKOTA
OPSEC AWARENESS
Quarterly Newsletter 2016

OPSEC & Your Home Network

Fundamental Practices to reduce your vulnerability:

- ***Change the default username and password often (90 days)***
- ***Don't stay logged in to the management website for your router***
- ***Turn the network off when not in use***
- ***Frequently update router firmware and patches***

Best Practices on Traveling With Your Smartphone

Before DEPARTURE

- **Save** all important data
- **Fortify** passwords
- **Update** software and apps
- **Encrypt sensitive** files
- **Delete** sensitive infor-mation
- **Enable** screen lock and timeout
- **Enable** Firewalls
- **Disable** Bluetooth and GPS
- **Leave** nonessential devices at home

During TRAVEL

- **Maintain** physical control always
- **Terminate** connec-tions after Wi-Fi use
- **Use** a VPN
- **Visit** secure websites only
- **Disable** file sharing
- **Avoid** public Wi-Fi networks
- **Never** use "remember me" for passwords
- **Don't** click links in text or email messages
- **Don't** download apps
- **Don't** connect to un-known devices

After RETURN

- **Avoid** immediately connecting device to personal or business networks
- **Scan** devices for mal-ware independently or through your organiza-tion
- **Change** all passwords

REMEMBER THE WINGS
100% SHRED POLICY

374 AW OPSEC Team
Capt Howell – 225-7811
Mr. Renteria – 225 8361

Interested in additional OPSEC training?

Please visit: www.iad.gov