M E M O R A N D U M

To: **Interested Parties**

From: **The Franklin Partnership**

Date: **December 3, 2019**

RE: ***Cybersecurity 101 Guideline***

A recent survey by the Small Business Administration found that "88 percent of small business owners felt their business was vulnerable to a cyber attack." Companies are also increasingly receiving requests from their customers that they have cybersecurity systems and protocols in place. While defense suppliers have long had certain compliance requirements, increasingly manufacturers are reporting additional mandates in customer contracts.

Cybersecurity concerns have expanded beyond simply email hacking and phishing scams. While financial exposure is still a major risk, increasingly attacks of corporate espionage and even sabotage are more common. Customers who transfer engineering design and product plans to job shops need verification that their intellectual property is secure in the hands of their suppliers.

This initial cybersecurity guideline document is to help you get started, provide additional resources, and help you meet your customers' requirements, including under Defense Federal Acquisition Regulation Supplement (DFARS) for Controlled Unclassified Information (CUI). While The Franklin Partnership is not a law firm or cybersecurity services company, enough clients have requested information, we felt it timely to provide a starting point for companies.

Our recommendation is to follow the strictest guidelines you can, which will allow your business to meet most customer requirements across a number of industries. Much of the below is adapted from W. Bush and Obama Executive Orders on Department of Defense and national security contractor cybersecurity requirements, mostly, Executive Orders 13556, 13636, NIST Special Publication 800-171, NIST Interagency Report 7621 Small Business Information Security, FCC Cybersecurityhub, among others. Additional resources and links to documents and training videos also appears below.

Please contact Omar S. Nashashibi (Omar@franklinpartnership.com) for more information.

Table of Contents

The Basic Top Ten Checklist for Every Company

1. Train employees in security principles: strong passwords, Internet use guidelines, penalties for violating company cybersecurity policies;
2. Protect against viruses, spyware, with latest security software, web browser updates;
3. Secure your Wi-Fi network, change passwords and set up router so it does not broadcast the network name (SSID);
4. Provide firewall security for your Internet connection;
5. Require employees to use strong passwords and to change them often;
6. Protect mobile devices by changing passwords, installing security apps, encrypt data, lost device reporting procedures;
7. Make backup copies of important business data and information;
8. Control physical access to computers, laptop locks, and user accounts for each employee;
9. Limit employee access to data and information, and limit authority to install software;
10. Protect all pages on your public-facing websites, not just the checkout and sign-up page.

A Few Key Top Ten Tips for Every Company

1. Even if you have an outside IT/security company, designate a single internal person to monitor your network, schedule password statements, and make sure employees agree to terms of use;
2. Force security system to require complex passwords, regular password changes;
3. Don't allow sites to "recognize this device", don't autostore passwords;
4. Don't collect personal information you don't need;
5. Apply locks to laptops;
6. Don't hold on to information longer than you need;
7. If an employee doesn't need access to customer, business, or personnel information, don't allow them access;
8. Develop a clear internet access policy, keeping in mind limitations on an employer's ability to restrict use of company internet access and devices once already permitted for personal use;
9. Require sign-in sheet at all shops for all guests;
10. Request certain guests not take cell phones (with recording devices) onto the shop floor;

The Basic Top Ten Tips While Traveling

1. Update your mobile software;
2. Back up your information;
3. Keep devices locked with complicated passwords, reset passwords upon return;
4. Disable Bluetooth;
5. Disable personal hotspot;
6. Do not connect to public wireless hotspot;
7. Do not click on links you don't recognize;
8. Don't insert a flash drive from an unknown source;
9. Avoid using hotel business centers as may have malware to capture your keystrokes;
10. Biggest cybersecurity concern is still physical theft, maintain control of your devices.

Implementing a Comprehensive Process also DoD DFAR Compliant

The Obama administration issued two executive orders updating previous requirements for the handling of unclassified information and incident reporting. The Trump administration, on January 27, released an additional FAQ that helps defense contractors comply with requirements and meet the December 2017 deadline to have systems in place. While many companies are not government contractors or supplying the defense industry, following these stringent and detailed guidelines are applicable across other industries as well.

Below is a very detailed itemized step-by-step checklist to comply with the DFARS Controlled Unclassified Information (CUI) mandate and set up a more secure process. For businesses not required to comply with defense contracting mandates, we suggest implementing the Basic Security Requirements listed under each subsection. Defense suppliers should consider implementing the Derived Security Requirements as well.

NOTE: All businesses should have their IT professional pay particular attention an increasingly common requirement under NIST SP 800-171 Section **3.5.3** "Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts." This added level of security can help assist in protecting business confidential information, including customers' intellectual property especially for those businesses using temporary employees.

3.1 ACCESS CONTROL

Basic Security Requirements:

3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
3.1.8 Limit unsuccessful logon attempts.
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.
3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
3.1.11 Terminate (automatically) a user session after a defined condition.
3.1.12 Monitor and control remote access sessions.
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
3.1.14 Route remote access via managed access control points.
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.
3.1.16 Authorize wireless access prior to allowing such connections.
3.1.17 Protect wireless access using authentication and encryption.
3.1.18 Control connection of mobile devices.
3.1.19 Encrypt CUI on mobile devices.

3.1.20 Verify and control/limit connections to and use of external information systems.
3.1.21 Limit use of organizational portable storage devices on external information systems.
3.1.22 Control information posted or processed on publicly accessible information systems.

3.2 AWARENESS AND TRAINING

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements:
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Derived Security Requirements:
3.3.3 Review and update audited events.
3.3.4 Alert in the event of an audit process failure.
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.
3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.
3.3.9 Limit management of audit functionality to a subset of privileged users.

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Security Requirements:

3.4.3 Track, review, approve/disapprove, and audit changes to information systems.
3.4.4 Analyze the security impact of changes prior to implementation.
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.
3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
3.4.9 Control and monitor user-installed software.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements:

3.5.1 Identify information system users, processes acting on behalf of users, or devices.
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Derived Security Requirements:

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.
3.5.5 Prevent reuse of identifiers for a defined period.
3.5.6 Disable identifiers after a defined period of inactivity.
3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.
3.5.8 Prohibit password reuse for a specified number of generations.
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.
3.5.10 Store and transmit only encrypted representation of passwords.
3.5.11 Obscure feedback of authentication information.

3.6 INCIDENT RESPONSE

Basic Security Requirements:

3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

Derived Security Requirements:

3.6.3 Test the organizational incident response capability.

3.7 MAINTENANCE

Basic Security Requirements:

3.7.1 Perform maintenance on organizational information systems.
3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Derived Security Requirements:

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in the information system.
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

3.8 MEDIA PROTECTION

Basic Security Requirements:

3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
3.8.2 Limit access to CUI on information system media to authorized users.
3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.

Derived Security Requirements:

3.8.4 Mark media with necessary CUI markings and distribution limitations.

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
3.8.7 Control the use of removable media on information system components.
3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.
3.8.9 Protect the confidentiality of backup CUI at storage locations.

3.9 PERSONNEL SECURITY

Basic Security Requirements:
3.9.1 Screen individuals prior to authorizing access to information systems containing CUI.
3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Derived Security Requirements: None.

3.10 PHYSICAL PROTECTION

Basic Security Requirements:
3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems.

Derived Security Requirements:
3.10.3 Escort visitors and monitor visitor activity.
3.10.4 Maintain audit logs of physical access.
3.10.5 Control and manage physical access devices.
3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

3.11 RISK ASSESSMENT

Basic Security Requirements:
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.

Derived Security Requirements:
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

3.12 SECURITY ASSESSMENT

Basic Security Requirements:
3.12.1 Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Derived Security Requirements: None.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements:
3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Derived Security Requirements:

3.13.3 Separate user functionality from information system management functionality.
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
3.13.10 Establish and manage cryptographic keys for cryptography employed in the information system.
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
3.13.13 Control and monitor the use of mobile code.
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
3.13.15 Protect the authenticity of communications sessions.
3.13.16 Protect the confidentiality of CUI at rest.

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements:

3.14.1 Identify, report, and correct information and information system flaws in a timely manner.
3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.
3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.

Derived Security Requirements:

3.14.4 Update malicious code protection mechanisms when new releases are available.
3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
3.14.7 Identify unauthorized use of the information system.

Cybersecurity Maturity Model Certification

Building on a clause from the DFARS, the Department of Defense is moving forward to adopt a framework for cybersecurity to better assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB).

The Cybersecurity Maturity Model Certification (CMMC) will review and combine various cybersecurity standards, such as NIST SP 800-171, NIST SP 800-53, ISO 270001, and ISO 2703, as well as best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced.

CMMC adds a verification component to the cybersecurity requirements in DFARS. CMMC also establishes a model framework with 17 different domains including access control, configuration management, identification and authentication, incident response, risk assessment, and system and information integrity. Each domain covers a key set of cybersecurity capabilities, and these capabilities contain practices and processes that are mapped to five numbered levels.

In general, contractors will be required to be certified by a DoD-accredited third-party auditor. All companies conducting business with the DoD, including subcontractors, must be certified. DoD will assess which CMMC level is appropriate for a particular contract and incorporate that level into the Request for Proposal (RFP) as a "go/no go" evaluative determination.

CMMC Levels

The CMMC model has five defined levels, each with a set of supporting practices and processes. Practices range from Level 1 (basic cyber hygiene) and to proactive and advanced Levels 4 and 5. To meet a specific CMMC level, an organization must meet the practices and processes within that level and below.

- Level 1 | Basic Cyber Hygiene (basic cybersecurity, achievable for all companies)
- Level 2 | Intermediate Cyber Hygiene (includes universally accepted cybersecurity best practices)
- Level 3 | Good Cyber Hygiene (coverage of all NIST SP 800-711 rev 1 controls)
- Level 4 | Proactive (advanced and sophisticated cybersecurity practices)
- Level 5 | Advanced/Progressive (highly-advanced cybersecurity practices)

DoD is planning to release Version 1.0 the CMMC framework in January 2020 and expects to incorporate CMMC requirements in RFPs beginning in June 2020.

Additional Resources, Toolkits, and Training Videos

Toolkit for Small and Midsize Businesses - C3 Voluntary Program
The Department of Homeland Security (DHS) and its partners have established a Critical Infrastructure Cyber Community (C3) Voluntary Program to help educate business owners about cybersecurity. The C3 Voluntary Program Toolkit for Small and Midsize Businesses contains resources to help your business recognize and address cybersecurity risks, including Fact Sheets for Startups and Leadership and a Hands-On Resources Guide. Learn more at https://www.us-cert.gov/ccubedvp/getting-started-smb. For additional tools and resources for small employers, visit http://www.dhs.gov/publication/stopthinkconnect-small-business-resources.

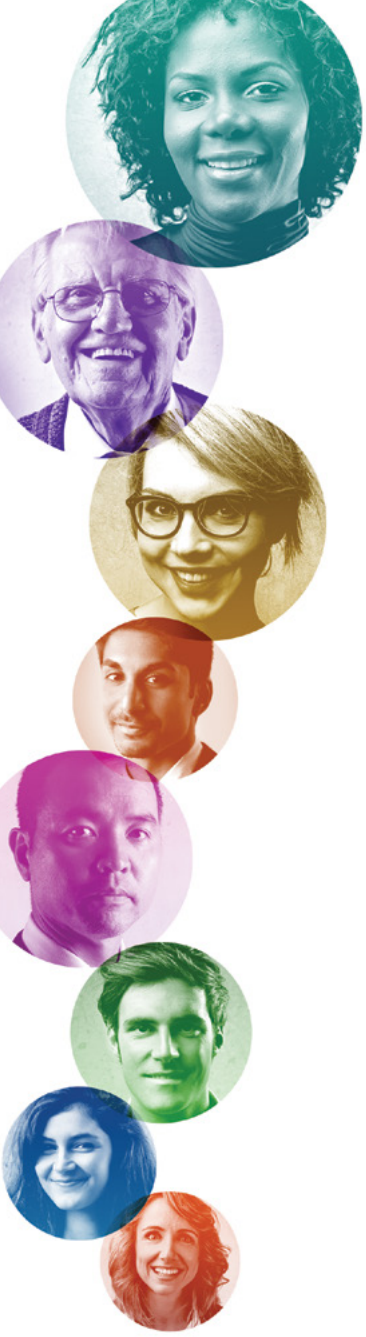
Small Biz Cyber Planner
The Federal Communications Commission (FCC), in collaboration with other government agencies and industry leaders, created the Small Biz Cyber Planner - an easy-to-use, free online tool that will help you create a customized planning guide to protect your business from cybersecurity threats. Learn more at www.fcc.gov/cyberplanner.

SBA Online Course: Cyber Security for Small Businesses
Cyber Security for Small Businesses will help you learn more about the security principles you should keep in mind when online, as well as the ways you can protect your information and networks in case of a cyberattack. For in-person assistance, visit your local SBA office or mentor**.**

Cyber Resilience Review (CRR) assessment tool
Developed by DHS, this no-cost, voluntary CRR assessment tool helps businesses assess their information technology resilience. The CRR evaluates ten domains including risk management, incident management, service continuity, and may be conducted as a self-assessment or as an in-person, facilitated assessment. For more information, visit https://www.us-cert.gov/ccubedvp/self-service-crr.

Cybersecurity Advisors (CSAs)
CSAs are regionally-located DHS personnel who offer immediate and sustained cybersecurity assistance to prepare and protect organizations, including small and mid-sized businesses. Services include on-site meetings to answer questions, exchange information and address concerns about cybersecurity; educational and awareness briefings; and assessments, including a full-day, expert-led a Cyber Resilience Review (CRR) evaluation that assess cybersecurity management practices. For more information about CSAs, please email cyberadvisor@hq.dhs.gov.

Local Resources
This collection of resources from various levels of government can help small and midsize businesses recognize and address their cybersecurity risks. Access resources in your area.



INDUSTRY EMPLOYEES TIP CARD

All employees play an important role within their organization. Each person must employ proper cybersecurity practices to ensure that all work-related information stays safe and secure. When each person makes a conscious and proactive effort to learn about cybersecurity, they enhance the company's ability to guard and protect the organization from vulnerabilities.

DID YOU KNOW?

- A combined **92 percent of human resource professionals** said increased vulnerability of business technology to attack or disaster will have an effect on the U.S. workplace in the next **five years.**[1]

SIMPLE TIPS

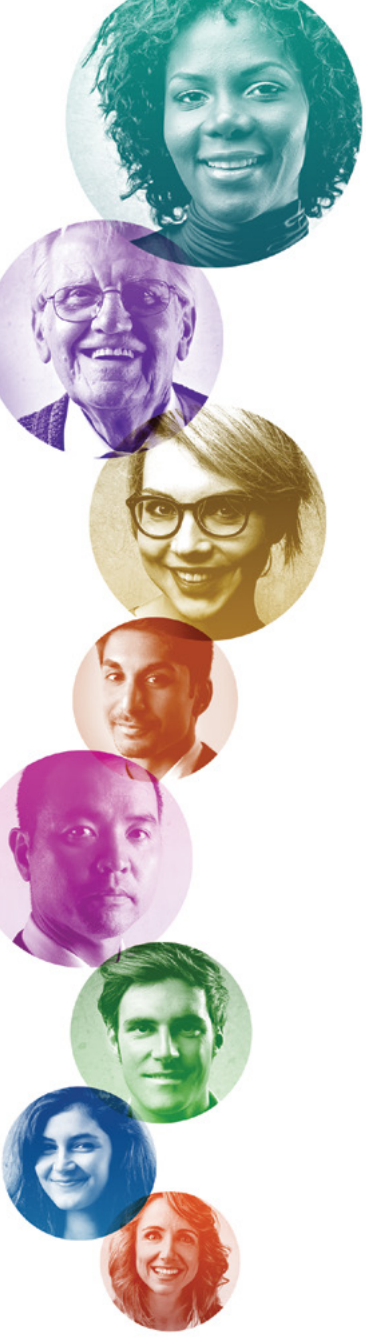
1. Read and abide by your company's Internet use policy.
2. Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
3. Change your passwords regularly (every 45 to 90 days).
4. Don't share any of your user names, passwords, or other computer or website access codes.
5. Only open emails or attachments from people you know.
6. Never install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
7. Make electronic and physical back-ups or copies of all your most important work.
8. Report all suspicious or unusual problems with your computer to your IT department.

RESOURCES AVAILABLE TO YOU

US-CERT.gov

The United States Computer Emergency Readiness Team (US-CERT) has numerous tips and resources on topics like choosing and protecting passwords, email attachments, and safely using social networks.

[1] SHRM, "SHRM Workplace Forecast: The Top Workplace Trends According to HR Professionals," 2013



FBI.gov

The Federal Bureau of Investigation leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber crimes.

CyberCrime.gov

Cybercrime.gov is the Department of Justice component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

IF YOU'VE BEEN COMPROMISED

- Report it to your manager or contact the IT or legal department to report the incident.
- Keep and record all evidence of the incident and its suspected source.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov, if applicable.
- Report fraud to the Federal Trade Commission at www.onguardonline.gov/file-complaint, if applicable.
- If someone has had inappropriate contact with you or a colleague, report it to www.cybertipline.com and they will coordinate with the FBI and local authorities. You can also report it to the Department of Justice at www.justice.gov/criminal/cybercrime/reporting.html.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and you community. For more information visit http://www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™