Cybersecurity

Cyber attacks against the government are increasing in frequency. The Office of the Comptroller is working with departments to build a stronger, more resilient system based on a network of informed staff.

All agency staff should receive training on best "cyber hygiene", as well as social engineering scams.

Given the ever-changing nature of cyber attacks, this training should be continuous.

Leadership should ensure that digital policies are in place and continually updated, and that fraud is included in any disaster recovery plans.

CTR CYBER HYGIENE FOR ALL USERS

- USE COMPLEX PASSWORDS
- RESTRICT ACCESS TO SENSITIVE DATA
- AUDIT USER ACCESS
- ALERT IT STAFF TO ANY SUSPICIOUS EMAILS
- INSTALL ONLY SOFTWARE APPROVED BY IT
- KEEP PASSWORDS OUT OF SIGHT
- KEEP INFORMATION ABOUT SECURITY MEASURES CONFIDENTIAL

The Office of the Comptroller provides a Cyber Center, compiled of useful resources to inform everyone about good cyber hygiene.

www.macomptroller.org/cyber-center

WHERE TO REPORT FRAUD

OFFICE OF THE COMPTROLLER

(617) 727-5000
ctremergencynotification@mass.gov

Contact the Statewide Risk Management Team to report agency cyber incidents, fraud, waste, or abuse.

OFFICE OF THE INSPECTOR GENERAL

(800) 322-1323

This confidential 24-Hour hotline can be used to report fraud, waste, and/or abuse in Massachusetts state government.

OFFICE OF THE ATTORNEY GENERAL

(617) 727-2200

Contact this office for data breaches covered by the Breach Notification Law (M.G.L. 93H) or other fraud complaints.

OFFICE OF THE STATE AUDITOR

(617) 727-8638

Report waste and abuse, state agency variances, losses, and shortages, thefts of funds, or property and public benefits fraud.

STATE ETHICS COMMISSION

(888) 485-4766

Contact the Commission for advice or with information about violations of conflict of interest laws.

WHISTLEBLOWER PROTECTION

Employees of the Commonwealth of Massachusetts are protected against retaliation for reporting violations of the law by:

M.G.L. c. 149, § 185 and M.G.L. c. 12A, §14(c).

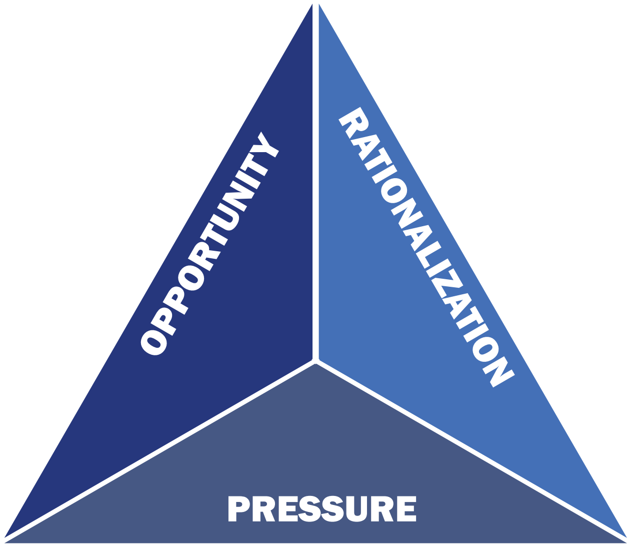
OFFICE OF THE COMPTROLLER
William McNamara, Comptroller
One Ashburton Place, 9th floor
Boston, Massachusetts 02108
(617) 727-5000
MACOMPTROLLER.ORG

Fraud Prevention: Everyone's Job

Tips for government agencies to fight fraud, waste, and abuse of public funds

> There is no kind of dishonesty into which otherwise good people more easily and frequently fall than that of defrauding the government.
>
> **Benjamin Franklin**

WHY DO PEOPLE COMMIT FRAUD?



THE FRAUD TRIANGLE

The Fraud Triangle is based on research by noted criminologist Donald Cressey. He hypothesized that trusted persons commit fraud when they convince themselves that they experience motivating pressure, see an opportunity to resolve that pressure, and are able to rationalize to themselves that the fraud is justified.

PRESSURE
Motivation to commit fraud,
especially personal financial pressure

OPPORTUNITY
Access to anything of value.
Examples include money, inventory, or data

RATIONALIZATION
Ability to convince self that fraud is justified

BE ON THE LOOKOUT FOR THESE COMMON TYPES OF GOVERNMENT FRAUD

- Falsified wages, overtime, or reimbursements
- Misdirected payments
- Ghost employees
- Fake vendors
- Invoices paid, but goods/services were not provided
- Conflict of interest in contracting
- Kickbacks or bribes
- Theft of cash or inventory
- Theft of Personally Identifying Information (PII)
- Fraudulent financial or programmatic reporting

RED FLAGS

These are symptoms of fraud, waste, and abuse occuring, but could also be a warning that conditions are ripe for them to occur:

- Poor Tone from the Top
- Lack of oversight and accountability for key functions, including cash, payroll, disbursements, credit cards, systems
- Employee or vendor banking changes
- Invoices or credit card charges without detailed backup
- Unusual expense reimbursements
- Unchecked overtime usage
- Undisclosed business relationships with vendors
- Unreconciled inventory (without physical count)
- Unauthorized access to automated systems

MOST KINDS OF FRAUD CAN BE PREVENTED

It all starts at the top.

Leadership must implement a Code of Conduct that meets or exceeds M.G.L. c. 268A, promoting the highest standards of ethical behavior, and consequences for committing fraud. All employees should be made aware of the Code of Conduct. Healthy organizations do the following:

- **ASSESS AND CONTROL RISK**
  Include fraud risks in an enterprise-wide risk assessment, in developing an internal control plan. Continually update and monitor these procedures to mitigate fraud risks specific to your organization.
- **BREAK IT UP**
  Segregate duties. No one person should be in charge of an entire process. Cross-train staff or rotate jobs.
- **WATCH THE LITTLE THINGS**
  Review unusual entries, significant deviations, overrides, and duplicate transactions.
- **SPREAD THE WORD**
  Fraud isn't just internal. Make sure vendors, grantees, sub-recipients and others are aware of their reporting responsibilities and liabilities.
- **WATCH THE LITTLE THINGS**
  Review documents and reconciliation for unusual entries or significant deviations from what's expected.
- **VERIFY BACKGROUND CHECKS**
  Make sure background check guidelines have been followed for employees and new hires.
- **TRAIN ALL STAFF**
  All employees should receive fraud prevention and cybersecurity training regularly.

The Office of the Comptroller regularly provides training to state agencies on cybersecurity and fraud prevention.

Call (617) 973-2468 to learn more.