CYBERSECURITY
is everyone's job.

Legal and Compliance

Understanding laws and risks

Legal implications drive compliance and mitigation efforts

Local government legal and compliance professionals have many titles — legal counsel, internal audit, risk manager, or attorney. Local governments often contract out for legal advice and counsel, leaving leadership and finance to make decisions about when to consult external legal counsel.

Here are three things you can do in your role to #BeCyberSmart.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated August 2019

As Legal and Compliance professionals, you play a necessary role in helping your government understand laws and risks. You also are key in mitigating those risks through implementation of an effective compliance program and creation of a holistic risk mitigation plan.

1 Educate yourself on the legal implications of cybersecurity

Your unique skillset enables you to effectively understand current and emerging cybersecurity-related laws, regulations and standards. It is essential that you stay current with cybersecurity and understand state, local and federal laws as well as industry standards.

Some cybersecurity requirements might have legal implications and consequences associated with non-compliance. A consequence could include fines associated with a data breach. You can help gauge your government's cybersecurity risk by asking yourself questions such as:

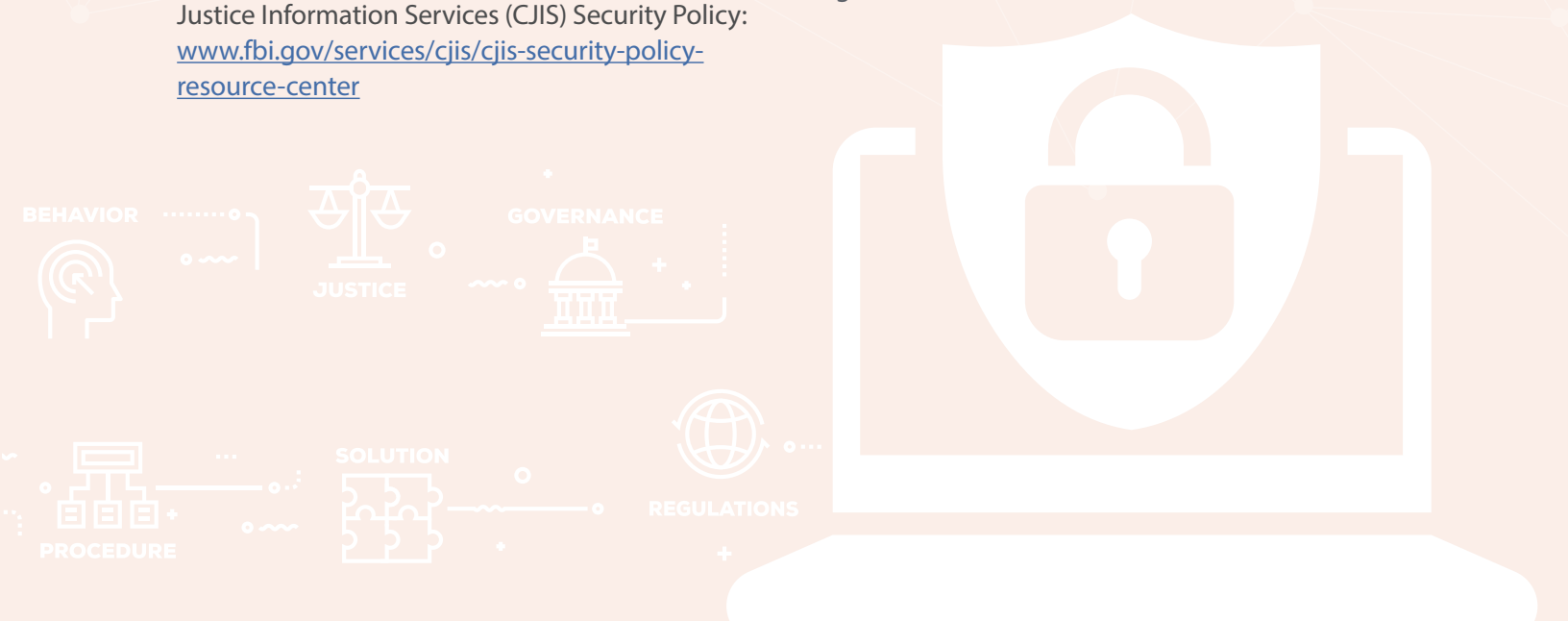
- **Does your government have health care information?** If so, you might be subject to the Health Insurance Portability and Accountability Act (HIPAA): www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

- **Does your government provide law enforcement services?** If so, you might be subject to the Criminal Justice Information Services (CJIS) Security Policy: www.fbi.gov/services/cjis/cjis-security-policy-resource-center

- **Does your government accept credit cards?** If so, you might be subject to Payment Card Industry (PCI) standards: www.pcisecuritystandards.org/pci_security/standards_overview
  A Self-Assessment Questionnaire tool is available to help you identify your PCI requirements: www.pcisecuritystandards.org/pci_security/completing_self_assessment

In addition, did you know that Washington has a data breach law? It is Revised Code of Washington (RCW) 42.56.590, and it defines personal information as well as details about the reporting requirements. View it at apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590

What other types of information does your government keep, and what kinds of compliance requirements do you have? Answering these questions will help you understand the laws, regulations and standards along with risks and potential liabilities that apply to your government.



2 Implement an effective compliance program

After your review of legal requirements and possible legal implications, you should begin to build your compliance program. Your program might vary from those of other governments, depending on the types of information you have and your applicable compliance requirements.

Establishing your policy on how to classify and access your local government's data and information is an important first step. This policy identifies how employees will know if they are using confidential information and how to protect that information from unauthorized access.

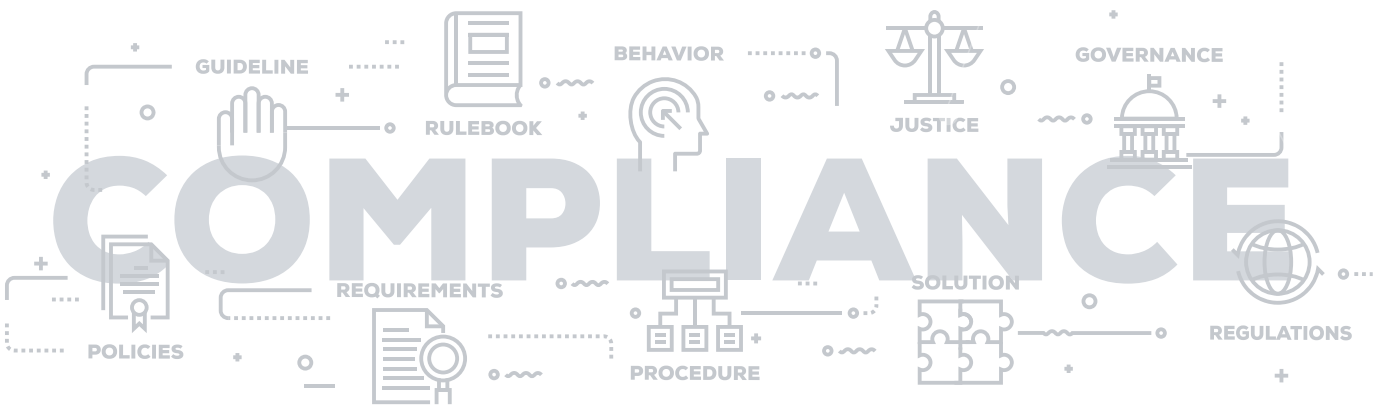
Policies should address helping employees know the difference between confidential information and public information. Employees should also understand the different methods used to store, protect and share information based on the level of confidentiality. For example, encryption is a tool that helps protect information when it is stored or shared. Here are some resources to help you develop your own policy:

- **State standards for Washington state agencies:** ocio.wa.gov/policy/securing-information-technology-assets-standards
- **Federal government standards:** nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

You can also use cybersecurity best practices to improve your compliance program, but you will need to work with your IT staff to accomplish this. Some best practice resources have controls or measures mapped to standards and regulations, like this one from the Center for Internet Security (CIS): www.cisecurity.org/cybersecurity-tools/mapping-compliance/

The CIS Controls represent a best practice that prioritizes a set of actions to protect an organization and its data, available at www.cisecurity.org/cybersecurity-best-practices/

After developing a policy, you will need to work with other departments in your local government to successfully implement it. Work together with your IT department to find out how to implement encryption. You should also work with your Human Resources department to develop training for employees based on the policy requirements. Ensuring that contracts with third parties (such as vendors or contractors) include clauses that define measures or controls to address cybersecurity concerns is a responsibility for each department in your government. Contracts should include prescribed cybersecurity clauses; ensure there is a monitoring mechanism in place for compliance. It's good practice for legal counsel to review contracts. For more information on contracts, you can view the "Finance and Administration" section of our #BeCyberSmart webpage.



3 Actively work across teams to create a holistic risk mitigation plan

Before you develop a plan to mitigate risks, you must first conduct a risk assessment for your entire local government that includes input from all departments. The risk assessment should include cyber-related risks. Legal and Compliance staff lend an important perspective in understanding the legal implications of various cybersecurity requirements and risk exposure. If you'd like more information about risk assessments, you can visit the "Leadership and Planning" section of our #BeCyberSmart webpage.

After completing the risk assessment process and identifying and prioritizing cyber-risks, work with other relevant departments to develop a plan for addressing those risks. Legal and Compliance staff are critical to developing and formalizing strategies for mitigating risks and reducing or eliminating legal exposure. Ideally, risk mitigation plans are documented and formalized to ensure all departments have a solid understanding of and mutual agreement regarding the steps to be taken. Follow up on this plan periodically to ensure risks have been reduced or mitigated as intended; the progress of your strategy needs to be measured and adjusted to stay effective.

You have an important role to play

As a Legal and Compliance professional, you help ensure your organization knows about and complies with legal requirements – including those related to cybersecurity. By starting with these three steps, and working with people in other roles in your organization, you can make a significant difference in developing a cybersecurity program that works for your government!

Our Office also offers training at conferences on cybersecurity. For upcoming dates and times, visit

sao.wa.gov/BeCyberSmart

Sources:

Department of Homeland Security
National Institute of Standards and Technology
Center for Internet Security

Center for Government Innovation