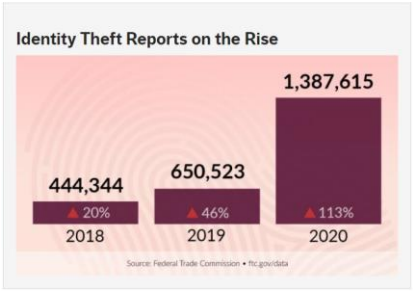
	Welcome on behalf of the California Department of Technology, Office of Information Security. This is "Protecting Privacy in State Government, Basic Training for California State Employees."
OUTLINE •Training goals •Why protect privacy? •Privacy laws for state government •Privacy practices for state employees	This is basic Privacy training for all state employees- keep in mind there could be additional training that many of you might be required or might want to be taking for specific job roles or for certain kinds of programs. Here's the outline… goals of this training, why we should be concerned about protecting privacy, and an overview of some of the major state privacy laws that apply to government agencies, and then, more of the presentation will be spent looking at privacy practices for state employees.
TRAINING GOALS •Learn consequences of mishandling personal information. •Consequences for individuals •Consequences for employees	As employees of Government agencies/state entities, we collect and store a lot of personal information on individuals, including Social Security numbers, taxpayer information, financial information, health, and medical information and more. As employees we must protect the data…This training is intended to make employees aware of their responsibilities and the consequences of mishandling personal information – - consequences for the individuals whose info is mishandled; And - consequences for state employees
TRAINING GOALS •Learn risky information-handling practices to avoid. •Recognize other such practices in your workplace. •Reporting information security incidents.	This training presentation will also provide awareness of some dangerous information-handling practices - and help you to recognize other risky practices in your workplace. Additionally, you will also learn when and how to report information security incidents in your workplace.

WHY PROTECT PRIVACY
• It's the law!
  • Information Practices Act, and others
• Security breaches
  • Highest average total cost exceeded $4 Million
  • Notifying affected individuals can cost over $200 per notice.
• Identity theft
  • The low-risk, high-reward crime of our times
	WHY PROTECT PRIVACY?
	First, it's the Law: State laws such as the Information Practices Act and depending on your agency/state entity's business function there are others that require state agencies to protect personal information
	And Security breaches are costly to the organization: For example, a lost laptop containing personal information – cost state agencies money (making reports of loss, replacement of the equipment, notifying all affected parties whose information was contained on the device, etc.) and loss of reputation and trust of public we serve. The annual Cost of a Data Breach Report, featuring research by the Ponemon Institute shows that in 2021 the average Data breach costs rose from 3.86 million to 4.24 million, the highest average total cost in the 17-year history of their report. Notifying affected individuals can cost over $200 per notice. One incident involving 100,000 individual's records x $200 per notice = $20M in notification costs alone.
	• Even an inadvertent personal information handling error incident, such as handing or sending out the personal information of one individual to another individual, can add up overtime if repeatedly occurring. $200 x 10 = $ 2,000 but $200 x 100 per year =$ 20,000 and $200 x 1000 per year = $200,000 and so on.
	AND we need to protect privacy from Identity Theft Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain. It's referred to as a low-risk, high-reward crime because thieves can easily commit the crime over the Internet from another local, state or country making law enforcement follow-up and attribution difficult. Any personal information is sought by identity thieves, who use it to harm people. It takes $800 on average for an individual to correct and undue the negative impacts of identity theft. However, personal harms are not only financial. We will discuss ID Theft in more detail shortly.

WHY PROTECT PRIVACY **Public Trust** • The public we serve often have no choice – they are required to provide personal information to government. • We have an obligation to protect the information entrusted to us.	Public Trust…People can't go to another DMV, another FTB, if they're not happy with the way their personal information is handled. People entrust their most sensitive personal information – financial information, medical information – to Government agencies. Our failure to protect personal information and use it properly can undermine Californians' faith in their government. More services offered in-person or online require state employees to diligently reduce risk to our customers personal identifiable information. Privacy in a Digital World is fast paced. Technological innovation is

	efficient and necessary, but we must ensure we don't let it outpace privacy protection.
IDENTITY THEFT What It is and Its Impact	Identity Theft – Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain. ID Theft has led to economic losses in the billions and more significant harms to individuals each year.
WHAT IS IDENTITY THEFT? •Obtaining someone's personal information and using it for any unlawful purpose •Penal Code § 530.5 •Financial •Existing accounts, new accounts •Services: Employment, Medical •Criminal	The most common type of identity theft is financial – thieves steal personal information and use it to make money. A thief may use a victim's existing account – such as a credit card account. Or a thief may use personal information such as name and Social Security number to open new accounts. Other kinds of identity theft include using someone's SSN to get a job – which can create tax liabilities for the victim. Or a thief may use someone's information to get medical benefits – which can cost the victim's insurer. This can also pollute the victim's medical records with the thief's diagnoses and treatments, putting the victim's health and life at risk. Imagine a victim having to visit the emergency room and need a blood transfusion and the blood type on their medical record is now incorrectly reflecting the thief's. "Criminal" identity theft is when a thief uses someone's information when arrested or charged with a crime, which creates a criminal record for the victim. This can be very difficult to correct and cause serious problems and harms until it is. For example, a victim could be arrested, held or imprisoned, slandered and lose out on prospective job opportunities until the matter is cleared up.
IDENTITY THEFT INCIDENTS 	Identity thieves were busier than ever as the pandemic erupted nationwide in 2020, with reports of identity theft in the U.S. skyrocketing to nearly 1.4 million in 2020, more than double the number a year earlier. The 2020 figures released by the Federal Trade Commission (FTC), a consumer protection agency, show from 2018 there were more than triple the number of identity theft reports in 2020. Cases climbed to just under 1.4 million (1,387,615) in 2020; up 113% from just over 650 thousand (650,523) in 2019; and 2019 up 46% from just over 444 thousand (444,344) in 2018.\

According to the 2021 Identity Fraud Study by Javelin Strategy & Research Identity fraud cost Americans $56 billion dollars in 2020. With 49 million consumers falling victim to identity theft. Increase stems from the Covid-19 pandemic. It changed the way people shopped and transferred money, many criminals targeted digital wallet and peer-to-peer payment methods such as Apple Pay and Zelle. About 18 million victims fell prey to scams through these digital payment methods in 2020, Javelin found.

About $13 billion in losses were due to what Javelin calls “traditional identity fraud,” where cybercriminals steal personally identifiable information and use it for their own gains, such as through data breaches. But the bulk of the $43 billion losses in 2020, stemmed from identity theft scams where criminals interacted directly with consumers to steal their information through methods such as robocalls and phishing emails. Victims of these scams lost $1,100 on average, according to Javelin.

And ultimately consumers are impacted – they pay those costs through higher prices for goods and services. Helping consumers and employees know how to spot the red flags of scams is an important step in stopping fraud before it has a chance to happen, and why employee security and privacy awareness training like this is so important.

A strong privacy program, which includes data security, is essential to the safety and welfare of the people of California and to our economy.

State government privacy laws

General Privacy Laws for All California State Agencies

STATE GOVERNMENT PRIVACY LAWS
• CA Information Practices Act of 1977
  • Civil Code §1798 et seq.
  • Includes breach notice law §1798.29
• CA Medical Information Confidentiality Act
  • Civil Code §1798.85-1798.86
  • Social Security Number Confidentiality Act §1798.85-1798.86
• Privacy Policies
  • Government Code §11019.9
	There are many state and federal privacy laws and regulations that state entities must adhere to. The California Information Practices Act (IPA) is the primary overarching privacy law applicable to ALL state government entities, with few exceptions. The IPA first established in 1977, requires state entities to provide a notice with the collection of personal information informing individuals about the purpose, use and maintenance of the information and includes the breach notification requirements for state entities, among other things. We will review each of its provisions in this training.
	Similarly, the California Confidentiality of Medical Information Act (CIMA) and the California Social Security Number Confidentiality Act applies to state entities. CIMA protects the medical history, condition, and treatment of ailments, including those related to transmitted diseases. The SSN Confidentiality Act requires the protection of SSNs in state government records and prohibits certain actions. I will provide more information about the SSN Confidentiality Act later in the presentation.
	There are also laws requiring all state government entities to have a published privacy policy on their website and posted in their facilities.
	In addition to these overarching privacy laws, which apply to all state agencies, there are also many other state laws protecting specific kinds of personal information such as vehicle license plate information and driver license information, and federal laws applying to certain state agencies.

INFORMATION PRACTICES ACT (IPA) • Comprehensive privacy law for all state agencies. • Sets requirements for agencies on collection and management of personal information.	We are going to walk through the IPA and its sections in more detail now. Section 1798.1, one of the Act's introductory provisions, captures the spirit of the legislation: "The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. "The IPA is a comprehensive privacy law applicable to all state agencies and it established requirements for personal information collection as well as management of personal information.

IPA: PERSONAL INFORMATION • Broad definition in IPA: "any information that is maintained by an agency that identifies or describes an individual," including, but not limited to: • Name, Social Security number, physical description, home address, home telephone number, education, financial matters, medical or employment history. It includes statements made by, or attributed to, the individual.	*Personal Information (Civil Code §1798.3)* • The IPA definition of "personal information" for purposes of the Act is very broadly defined to mean any information that is maintained by an agency that identifies or describes an individual, **including, but not limited to,** his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. • definition of personal information provides not just the very sensitive personal information types such as SSN, medical, and financial, but it also includes the kind of information that ID thieves are after such as home address & phone number, employment, and education history, etc. The more information they have access to, the more harm they can do. • The definition is more narrowly defined for purposes of the breach notification requirement which will be discussed later in this training.
IPA: INDIVIDUAL ACCESS TO PERSONAL INFORMATION • Individual has the right to see, dispute, correct his or her own personal information.	• Individuals have the right, under the Information Practices Act, to see the records government maintains about them – and the right to dispute and correct their records if in inaccurate. • The IPA permits individuals to access personal information state agencies maintain in files and records about them, unless they are specifically exempt. The IPA also restricts the disclosure of an individual's personal information to members of the public. Redaction of personal information is required when other parts of a record are considered public. Some examples of records exempt from disclosure to even the individual data subject include but are not limited to: • Criminal investigation records • Certain employee records • Testing or examination criteria • Personal information relating to another person, which would violate their privacy

IPA: SECURITY OF PERSONAL INFORMATION •Must protect personal information against risks such as unauthorized access, modification, use, destruction. •Use reasonable security safeguards: administrative, technical, physical	The IPA requires state agencies to protect personal information from unauthorized access, use, modification, and destruction. • Agencies must use reasonable and appropriate safeguards to protect personal information such as; Administrative safeguards – such as policies on use of passwords for access to databases Technical safeguards – such as firewalls and encryption of data Physical safeguards – such as locked file cabinets, buildings with card key-controlled access We'll cover some other examples of practices for safeguarding personal information later in the training presentation.
IPA: ACCOUNTABILITY •Individuals may bring civil action vs agency •Intentional violation by employee is cause for discipline, including termination •Willfully obtaining record containing PII under false pretenses is misdemeanor •Up to $5,000 fine and/or 1 year in jail	Accountability… • There are *consequences* for violating the Information Practices Act. • Consequences for **an agency** – which may be sued, if violation results in adverse impact. • Consequences for **an employee** – if the violation is intentional. • Also, consequences for an employee who obtains personal information under false pretenses - • Misdemeanor, punishable by a fine of up to $5,000 and one year in jail
IPA: NOTICE OF SECURITY BREACH •Agencies must notify people promptly if certain personal information is "acquired by unauthorized person."	Notice of a security breach is part of the Information Practices Act for state agencies/entities Agencies/state entities are required to operate in accordance with a myriad of laws and state policies related to the protection of information assets, and the timely and efficient management of information security incidents. California's breach notification law (Civil Code Section 1798.29), enacted in 2002, is one such law, intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so they could take steps to protect themselves against identity theft or to otherwise mitigate the crime's impact and other possible harms associated with a breach of personal information. Requires notification of individuals if their personal information – of a specific type – is "acquired by an unauthorized person" – or is reasonably believed to have been acquired. Intent of law is to give people early warning when their personal info has been compromised – to give them

	opportunity to take steps to protect themselves against ID theft. For example, if your SSN is involved in a breach, you can place a fraud alert or security freeze on your credit files, protecting you from new accounts being opened using your information.
BREACH NOTICE LAW Personal info triggering notice: An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: • Social security number • Driver's License number, California identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.	Generally, the kind of personal information that triggers the notice requirement is the kind identity thieves want. The breach notification section of the IPA, subdivision (g) of Civil Code Section 1798.29, more narrowly defines, "personal information" as the following…An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social security number. READ list on slide. Cont'd on next slide…
BREACH NOTICE LAW • Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. • Medical information • Health insurance information.	READ LIST ON SLIDE (continued next slide)
BREACH NOTICE LAW • Genetic Data • Automated license plate recognition system, as defined in Section 1798.90.5., and • A username or email address, in combination with a password or security question and answer that would permit access to an online account.	READ LIST ON SLIDE (continued next slide)

BREACH NOTICE LAW

- Applies to "unencrypted, computerized" data
- State policy is to notify in cases of breaches of notice-triggering information, no matter what format
  - Paper and digital data

The Breach notification law applies to "unencrypted, computerized" data.

- Encrypted means coded or scrambled so that it's not readable except by those who have a key.

State policy for state agencies is to notify in case of breaches involving "notice-triggering" personal information – in any format – paper, electronic, tape, etc.

- The risk to individuals is same, whether their data was on paper in a manila folder or in a database on a computer.
- You will find State policy Authority is in the State Administrative Manual (SAM) 5350.4, Information Security Incident Management and Statewide Information Management Manual (SIMM 5340-C Requirements to Respond to Incidents Involving a Breach of Personal Information.
- SIMM 5340-Cprovides information to ensure compliance and consistency across state government, this document identifies the current breach notification requirements for breaches involving personal information, accompanied by questions and factors agencies/state entities should consider in determining whether and when a breach notification should be made, and a specification of the means for fulfilling notification requirements.

PRIVACY AND PUBLIC RECORDS

- Personal information is protected, even in records that are public.
  - State agencies redact personal info before releasing public records.
  - Check with your PRA coordinator or with Legal.

The next topic is Privacy and Public Records. Records can be public – but personal information in the records is still protected – which is why state agencies redact personal information.

The **California Public Records Act** (PRA) is a series of laws designed to guarantee that the public has access to public records of governmental bodies in California. When the law was passed, the California legislature prefaced it by saying, "...access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state. "

There are certain categories of personal information and records that are exempt from disclosure under the PRA such as Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy. And there are also state laws which protect individual privacy interests and other propriety information from disclosure, including the federal Health Information Portability and Accountability Act (Public Law 104-191 as amended), and the Uniform Trade Secrets Act (Civil Code section 3426). Your agency/entity should have specific policies for such Public records requests…always check with your

	department's Public Records Act coordinator or Legal office before providing any information.
SSN CONFIDENTIALITY ACT •Prohibits "publicly posting or displaying" of Social Security Number, including: •Printing SSN on ID/membership cards •Mailing documents with SSN to individual, unless required by law	I mentioned the Social Security Number Confidentiality Act briefly a little earlier in the training. Let me share more specifics – The SSN Confidentiality Act requires the protection of SSNs in state government records and prohibits certain actions. such as, among other things: -publicly posting or publicly displaying an SSN in any manner, or -printing an individual's social security number on any card required for the individual to access products or services provided, or -printing an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed, or As you can imagine this was a huge undertaking for certain state entities – for some govt entities that provide Identification cards with SSNs printed on ID cards for access to goods or services. You may recall your health insurance cards had your SSN.
SSN CONFIDENTIALITY ACT •Requiring an individual to transmit over the internet only if the connection is secure or the SSN is encrypted •Requiring password or unique personal identification number or other identification device for website access	-requiring an individual to transmit the individual's social security number over the internet, unless the connection is secure or the social security number is encrypted, or -requiring an individual to use the individual's social security number to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website
RECOMMENDED PRIVACY PRACTICES Basic Practices for State Employees	There are some basic practices for handling personal information responsibly so that it is protected from unauthorized access and use. These practices are appropriate for most – but not all – work environments. They are intended to make you aware of safer – and of less safe – ways to handle the personal information that you come into contact within your job. Okay, let's talk about the basics!

CONFIDENTIAL INFORMATION •Personally identifying information - one type of information to protect •Other confidential information to protect includes security-related info, policy drafts, and some department financial information	Information is an asset and, like other business assets it is essential to your agency. Information can exist in many forms. It can be printed or written on paper, stored electronically, sent via post office or transmitted using electronic means, shown on monitors, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always by appropriately secured. Collecting and maintaining personal information presents increased risk and therefore increased responsibility. Protecting personal identifiable information (PII) protects individuals' privacy. Agencies must also protect other kinds of confidential information – such as computer security information and department banking information. Practices described here are intended to protect personal information – but they would also protect other kinds of confidential state information.
PERSONAL INFORMATION = MONEY •Handle personal information like it's cash!  	Personal information is worth money – There's a black market for personal information and identity thieves use it to make money. If you thought of personal information as cash, you would probably handle it differently. You wouldn't leave a pile of $100 bills lying on your desk so protect PII when you're away even just for a short meeting, for example. This is how we should all think of the personal information in our care.
KNOW WHERE PERSONAL INFORMATION IS •Learn where personal info is stored in your office – especially sensitive info like SSN, DL number, financial account number, medical information •PCs, workstation file drawers, laptops, mobile device, other portable devices •Employee info as well as information of consumers, licensees, others.	Know where personal information is…. Where do you store downloaded personal identifiable information? Your laptop or computer? Is it only in a specific drive within your department's network? For those business functions that continue with paper process --- Do you have printouts of personal information in file folders in an unlocked drawer in your workstation? The first step to protecting personal information is to know where it is. Take time to assess where you may be leaving PII at risk. And take this as a time to ask where the information SHOULD BE STORED.

RETAIN ONLY WHEN NECESSARY •Regularly purge unneeded duplicates with personal info from file folders. •Unless required to keep. •Avoid downloading onto PCs. •Regularly remove personal info from PCs, laptops, other portable devices. •Comply with record retention policy for official files.	When you've started to locate where you're keeping personal information in your workstation – consider whether you really need to keep it all. There are some kinds of records and data that we're required to keep, for legal reasons. But there are probably lots of other files – paper and digital – that we no longer need, don't need to keep – and SHOULD NOT keep beyond the period when we're working on them. Develop the habit of regularly purging documents containing personal information from your file folders. Avoid downloading from databases onto your PC – regularly delete what you do download when you've finished using it. Comply with your departments record retention policy for official files.
DISPOSE OF RECORDS SAFELY •Shred documents with personal information & other confidential information before throwing away. •Have computers and hard drives properly "wiped" or overwritten when discarding. •Lock up Confidential Destruct boxes when left unattended.	When you have identified what documents are no longer required or needed, don't throw documents containing personal information into your waste basket or recycling bin. If there is a shredder, then please shred them first. In the past several years state entities have been provided large containers for confidential information so be sure to utilize them. These containers are not for data storage media items such as flash drive so consult your department's Information Security Officer about disposing of other data storage media.
PROTECT PERSONAL INFORMATION FROM UNAUTHORIZED ACCESS •Limit access to personal info to those who need to use it to perform their duties. •Minimum necessary access	Protect Personal Information from Unauthorized Access. Be mindful of workload and responsibilities ---Not everyone in an office NEEDS to have access to all files and databases containing personal information. Especially info like SSN, DL number, financial account number, medical info. Don't give your access to co-workers or others who are not authorized. Depending on your role you are the employee who should often review who has access to PII or are the employee who can provide information to a manager or supervisor informing of unnecessary access concerns.
PROTECT PERSONAL INFORMATION IN WORKSTATIONS •Adopt "clean-desk policy": Don't leave documents w/ personal information out when away from workstation. •Lock up documents overnight and on weekends. •Lock PC when away from workstation.	Protecting Personal Information in workstations. No matter where your workstation is located remember to treat personal information like cash – don't leave it sitting out on your desk when you're away. Put files containing personal information in locked drawers or cabinets overnight. Lock your PC when you walk away – Remember "Control, alt, delete"

PROTECT PERSONAL INFORMATION IN WORKSTATIONS

- Never download "free" software onto PC – may contain spyware
- Passwords - use strong passwords
  - 8+ characters, a mix of letters (upper and lower case), numbers and symbols

Free software may not be free – It may contain spyware that can

- impair the operation of your computer,
- carry malicious programs that can steal your passwords and data, or
- introduce a virus into your department's system.

Check with your IT department before loading any software you think you need.

And protect access to your computer - Don't use obvious facts or numbers as your password – nor spouse's or child's name, or birthdate.

- Use combination of numbers, letters, symbols – 8+ characters
- One way to create a memorable password that others can't guess is to use initial letters of a sentence that has meaning to you – substituting numbers for some letters and adding symbols.
  - I.e., My favorite color is purple = mfc1p&

And leave the post it notes for actual notes and not your password stuck to your computer monitor or under your keyboard. ☺ And don't share it with others.

PROTECT PERSONAL INFORMATION ON MOBILE COMPUTING DEVICES

- Personal info on laptops, flash drives, other mobile computing devices must be **encrypted.** (policy for state agencies)

Mobile technology increased flexibility for employees, and it also increased security needs. Mobile devices are susceptible to many of the same vulnerabilities as personal computers so state entities and employees must make sure to adhere to state policy. State gov't policy requires that personal information (especially SSNs, DL/ID numbers, financial account number or medical info) on laptop or other portable computing device or storage device like flash drive – MUST BE ENCRYPTED.

Authority: SAM 5345.2 - Encryption on Portable Computing Devices

How vulnerable? Nearly half the security breaches requiring notification in recent years have involved lost or stolen laptops or other portable devices. Always know where you computing device is…Do not leave it unattended – use strong passcodes for mobile devices and keep them locked when not in use. The mobile devices are expensive and the PII that can potentially be obtained from an unencrypted device is far more expensive.

When personal information on portable devices is encrypted, it *can't* be accessed or used by an unauthorized person.

PROTECT PERSONAL INFORMATION IN TRANSIT •Any PII should be encrypted. If not, do not send via email. •Don't leave personal info in voice mail message. •Mail securely. •Don't leave incoming or outgoing mail containing PII in unlocked or unattended receptacles.	Protect Personal information in transit…. Think of email as a post card – Don't send personal information or other sensitive information by email – It's not a secure medium. Easy to send to the wrong person, dept, etc. • If your business function requires PII, make sure to follow your department's security and privacy policies…There are procedures for encrypting email and if you are not sure ask your manager or supervisor or your Information Security Officer. Don't leave personal information in a voice mail message – you don't know who might pick up the message. Or there are instances where you may accidentally misdial and leave a voicemail message containing confidential information for someone else to hear. Leave only contact information instead. Mail thieves are often after personal information. Don't leave outgoing mail unattended – lock it away when leaving the area. Same for incoming mail. It's not safe to have mail containing checks or other documents containing SSN's, account numbers, etc., delivered to a department on a Saturday. This is an opportunity for thieves and will result in a breach notification via news media and website because the department will not know whose mail was stolen therefore an individual notice is not possible.
PROTECT PERSONAL INFORMATION IN TRANSIT •Don't send sensitive info by fax, unless security procedures are used •Confirm accuracy of number before keying in •Arrange for and confirm prompt pick-up	How about faxing information? Yes, there are still fax machines and faxing is still a way to transmit information. Faxing can be insecure – don't know who will see or pick up fax from machine. Also, it's easy to mis-key and send to the wrong person. If you must fax personal information do so with caution and be sure to: • Confirm number and key in carefully • Call recipient to notify of fax and get confirmation of prompt pick-up. • Print outs are available that state the fax was successfully transmitted and the fax number. So, VERIFY and VALIDATE. If it was sent to the wrong number, then you must report the incident.

PROTECT STATE INFORMATION IN TRANSIT •Don't take or send State records with personal or confidential info home unless authorized. •If authorized, use only State laptop or other State equipment.	Unless you are authorized by your supervisor or manager, don't take or send State records containing personal information home. If you are authorized to work on state records at home, do so only on State computer equipment as a home computer may not have appropriate security protections, and it may be used by others who are not authorized to see state records. While working from home or telework or working remotely…recognize the risks of having your state mobile computing devices which may contain PII data unprotected. Follow the same in office guidelines or adopt even stricter guidelines due to other risk factors such as home break-ins resulting in computer and mobile devices being stolen. The recent increase in working from home has brought an increase in awareness for employees to protect and guard data. There is policy and guidance in the SIMM 5360-A, Telework and Remote Access Security Standard as well as the Statewide Telework Policy, SAM Section 181 which was issued October 2021. The purpose of the Statewide Telework policy is to provide the structure needed for effective telework programs to benefit the state of California and its employees. Each department shall establish a written policy specific to the department's business needs in accordance with this statewide policy. While employees and state entities navigate current, and future of "the workplace" ensure employees utilize the Statewide Telework Policy to develop internal technology policies and/or guidelines that are department specific. Those department-specific technology policies and/or guidelines shall include, but not be limited to: 1. Sufficient internet bandwidth required to perform duties. 2. Standards and expectations for communication and collaboration tools. 3. Security requirements for state-owned and for employee-owned computing devices (if allowing teleworkers to use them). 4. Physical and electronic data protection and 5. Asset Management.

DON'T BE FOOLED •Identity thieves may try to trick employees into disclosing personal information. •Phishing e-mails, phone calls •Verify identity and authority of anyone requesting personal information.	Identity thieves often try to steal confidential information by lying and manipulating someone into providing it. One common form is what's known as "phishing" – an email that looks like it's from a bank or a government agency, for example, asking you to confirm your password, account number, or Social Security number – claiming to part of an effort to protect you from fraud. • The advice to consumers in light of phishing – which takes place over the phone as well as by email – is NEVER give out your personal information unless you initiated the contact. Such schemes are also targeted at businesses and gov't agencies – relying on workers' desire to provide good customer service. • When you get a request for personal information on individuals from someone you don't know, make an effort to verify the identity and authority of the requester. • If you're not sure, check with your supervisor or manager for your department's policy/process for such requests. If you have questions about the applicability of any of these recommended practices in your workplace, please raise the issue with your supervisor or with your department's Information Security or Privacy Officer.
REPORT INFORMATION SECURITY INCIDENTS •Reportable incidents include: •Loss or theft of mobile computing device or portable media device. (laptop, cell phone, etc.). •Loss or theft of paper records •Unauthorized acquisition of protected information. •Unauthorized release, modification, or destruction of protected information.	Reporting Information Security Incidents…to be able to maintain good information security – to protect the information people give to us – departments must know about how to report information security incidents promptly. Be alert to incidents that could expose information to unauthorized access, disclosure, modification, or destruction. Such an incident could be • Lost or stolen laptop, mobile device, or any portable media, etc. • Lost or stolen mail containing documents with Personally Identifiable Information (PII), or other records contain PII • Improperly disposed of documents • An unauthorized person getting access to information [Next slide is about reporting incidents.]

REPORT INFORMATION SECURITY INCIDENTS •Report **any** security concerns or incidents immediately. •Allow management and your Department's Information Security Office to determine extent and significance.	**It is important to be familiar with your department's procedures for reporting a security incident.** Report any information security incident PROMPTLY to your department's Information Security Office. • Even if you're not sure an incident involves personal information. • Your ISO will determine the extent and significance of the incident. Of course, report the incident to your supervisor or manager. **Over-report,** rather than under-report, potential incidents. And prompt reporting is essential. The sooner an incident can be investigated, the sooner any security holes can be filled.
A MATTER OF RESPECT •Respect for citizens and co-workers means protecting their personal information. •Protecting privacy is everyone's responsibility.	A Matter of Respect. Protecting privacy is a matter of respect – • Respect for our fellow citizens who entrust us with their personal information, and • Respect for our co-workers, whose information is also in your department's care. Protecting personal information is something an Information Security Officer or a Privacy Officer can't do alone. As state employees we all touch some of the personal information in our offices and we are all responsible for protecting it.
PRIVACY QUIZ Quiz Time!	The Privacy Awareness training is complete, and it is now time to test your privacy knowledge. The presentation and quiz slides are available for your department to utilize in the format which is best. You can choose to end here and offer the quiz questions separately or continue with the presentation. If the choice is to continue with the presentation is the option…let's continue.
QUIZ QUESTION 1 A Public Records Act request is made for a state government document that contains the home addresses and Social Security Numbers of several people. Which one of the following statements is true?	Read slide

OPTIONS FOR Q1 a) The document is public and must be provided as is to anyone who makes a PRA request for it. b) Because the document contains personal information, it isn't public and should not be given in response to a PRA request. c) The document may be provided in response to a PRA request, but only after the home addresses and SSNs have been redacted. d) The document is not a public record if you created it on your PC for your own use in doing your job.	Read slide
CORRECT ANSWER TO Q1 c) The document may be provided in response to a PRA request, but only after the home addresses and SSNs have been redacted.	The correct answer is c) The document may be provided in response to a PRA request, but only after the home addresses and Social Security numbers have been redacted. Check with your supervisor or your department's PRA Coordinator on any PRA request. The requirements of the Public Records Act and the Information Practices Act must often be balanced. Redacting personal information in public records is one way to do this. Note – Option D…the fact that you created the document for your own use in doing your job does NOT prevent it from being a public record. Government Code §6252 (e) "Public records" includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.
QUIZ QUESTION 2 If you believe that incoming mail has been stolen from your office, where should you report it FIRST?	Read slide

OPTIONS FOR Q2 a) To your supervisor. b) To your department's Information Security Officer (ISO). c) To the U.S. Postal Inspection Service. d) To the local police department.	Read slide
CORRECT ANSWER TO Q2 b) To your department's Information Security Officer (ISO).	The correct answer is b) To your department's Information Security Officer. You should also report the mail theft to your supervisor. But in order to ensure that a possible security breach is handled promptly, let your ISO know about any information security incident as soon as you discover it. The ISO will coordinate and handle any additional reporting to appropriate authorities.
QUIZ QUESTION 3 Which of the following is the strongest – most secure – password for access to your PC?	Read slide
OPTIONS FOR Q3 a) FLUFFY b) 9151950 c) ERICKSON d) HMWC1WC?	Read slide

CORRECT ANSWER TO Q3 d) HMWC1WC?	The correct answer is d) HMWC1WC? A strong password such as those that contain at least 8 characters, including numbers and symbols. Remember Weak passwords are those that are easy to guess - passwords include pet names, birth dates or anniversaries, and your mother's maiden name. This one is based on the first letters of the words in the sentence "How much wood could a woodchuck chuck?" It's something you can remember but it's difficult for others to guess. Lyrics from favorite songs or a phrase with numbers and symbols also make for strong passwords.
QUIZ QUESTION 4 Which of the following is the most secure way to get the SSNs of 7 people to a co-worker, who is on a business trip, is authorized to have the information, and needs it to do his/her job?	Read slide
OPTIONS FOR Q4 a) Send the information in an e-mail. b) Call your co-worker and provide the information over the phone. c) Leave the information in a voice mail message on your co-worker's cell phone. d) Fax the information to your co-worker at the hotel.	Read slide
CORRECT ANSWER TO Q4 b) Call your co-worker and give the information over the phone.	The correct answer is b) Call your co-worker and give the information over the phone. Calling your co-worker is the best of the alternatives. Email is not a secure communications channel, because it can be hacked into as it passes over the Internet. Voice mail is generally not secure because other people may pick up the message. Faxes, especially to a public fax machine like a hotel's, are also not secure. Note that the employee is authorized to have this information, which is the first issue to consider.

QUIZ QUESTION 5 TRUE OR FALSE: If you delete files from your PC – and empty the recycle bin – that means the data in the files is erased.	Read slide
CORRECT ANSWER TO Q5 False	The correct answer is FALSE Erasing data from a computer does not completely remove it. Special overwriting software must be used to properly "wipe" a hard drive. Check with your Information Security Officer before disposing of any computer hardware.
QUIZ QUESTION 6 Which of the following would NOT be an information security incident to report to your department's Information Security Officer?	Read slide
OPTIONS FOR Q6 a) Loss of a laptop containing unencrypted or encrypted information. b) Accidental mailing of an individual's medical records to the wrong person. c) Theft of your purse, which contained a flash drive with state data on it. d) Theft of a state-owned electric stapler.	Read slide

CORRECT ANSWER TO Q6 d) Theft of a state-owned electric stapler.	The correct answer is d) Theft of a State-owned electric stapler. All of the other incidents involve data, which may include personal information or other confidential information. The theft of the stapler should be reported to your supervisor as a theft of state equipment.
QUIZ QUESTION 7 Which of the following should you do before you leave your workstation for a meeting?	Read slide
OPTIONS FOR Q7 a) Put documents, flash drives, other records containing personal information in a drawer and lock it. b) Hit “control-alt-delete” and lock your computer. c) Put your personal belongings which contain PII in a drawer and lock it. d) All of the above.	Read slide
	The correct answer is d) All of the above. Even when leaving your workstation temporarily during the day, lock your computer by (“control-alt-delete” and lock) to protect the data on it, and put paper records, flash drives and any other storage media away out of sight. When you are finished for the day, lock or shut down your computer as well as lock up all other data.

CORRECT ANSWER TO Q7 d) All of the above. • Put documents, flash drives, other records containing personal information (including your purse) in a drawer or otherwise out of sight. • Hit "control-alt-delete" and lock your computer.	
QUIZ QUESTION 8 A state employee gives a printout of the names, addresses, and driver's license numbers of people who received unemployment benefits to a friend who wants to offer jobs to them. Which of the following are true?	Read slide
OPTIONS FOR Q8 a) The employee could be found guilty of a misdemeanor punishable by up to $5,000 and sentences to one year in prison. b) The employee could be disciplined or fired. c) The employee's department could be sued. d) The employee will not be punished because his intentions were good.	Read slide
CORRECT ANSWER TO Q8 a) The employee could be found guilty of a misdemeanor punishable by up to $5,000 and sentenced to one year in prison. b) The employee could be disciplined or fired. c) The employee's department could be sued.	The correct answers are a), b), and c). The Information Practices Act contains penalties and consequences for those who violate it. Giving this kind of personal information to an unauthorized person places individuals at risk of identity theft, among other things. a) The employee could be found guilty of a misdemeanor punishable by up to $5,000 and one year in prison as stated in Civil Code §1798.56. Any person who willfully requests or obtains any record containing personal information from an agency under false pretenses... b) The employee could be fired as stated in Civil Code §1798.55.

	c) The employee's department could be sued as stated in Civil Code § 1798.45.
QUIZ QUESTION 9 TRUE OR FALSE: A folder containing job applications, which include the applicants' Social Security numbers, is stolen from a State employee's car. The employee's department does not have to notify individuals of this, because the information was not in digital or computerized format.	Read slide
CORRECT ANSWER TO Q9 False	The correct answer is False. An agency/state entity must notify the job applicants as the applications contained their PII such as first and last names, addresses and employment information, etc. Note: Never leave "CASH" (Personal Identifiable Information) in your car unattended and avoid leaving cash in a locked trunk.
QUIZ QUESTION 10 TRUE OR FALSE: Cyber criminals only target large companies.	Read slide

CORRECT ANSWER TO Q10 False	The correct answer is False. Cyber criminals target government entities of all sizes as well as companies of all sizes. Stay alert and do your part to reduce risk of data getting into the wrong hands.
PRIVACY RESOURCES • California Privacy Laws, Consumer Information and Identity Theft Informatio at: https://oag.ca.gov/privacy/ • California Department of Technology, Statewide Policies and Guidelines at https://cdt.ca.gov/policy/simm/ and Department of General Services State Administrative Manual at https://www.dgs.ca.gov/Resources/SAM/TOC/5300 Consumer Privacy Resources Identity Theft Protecting Children Online Business Privacy Resources Privacy Enforcement, Laws, and Legislation Privacy Reports Special Protection Data Breaches	Before I conclude the training, I want to share resource information…. State policies, Statewide Information Management Manual (SIMM's) are available on the California Department of Technology Website and the State Administrative Manual (SAM) policies on the Department of General Services website. The Office of Attorney General Website is another resource for Privacy Laws, Consumer Information, and Identity Theft. Additional information on OAG website [read right margin of slide]…Consumer Privacy Resources, Identity Theft, Protecting Children Online…. In the 21st century, we share and store our most sensitive personal information on phones, computers and even in "the cloud." Today more than ever, a strong and privacy aware workforce is essential to the safety and welfare of the people of California and to our economy. Stay aware! This State Employee Privacy Awareness Training is available for state entities on the California Department of Technology website under Security, and then click on Privacy Management. This recorded presentation, PowerPoint presentation for facilitator (with speaker notes), document with all slides as well as guidelines to assist with providing this training. The guideline document also contains a sample template of a Privacy Awareness Training Acknowledgement Form. Thank you for attending.