

Computer Laws and Acts

Table of Contents

Fair Credit Reporting Act.....	2
Privacy Act of 1974	4
Counterfeit Access Device & Computer Fraud & Abuse Act - 1984	6
Electronic Communications Privacy Act	9
Computer Fraud and Abuse Act.....	11
Computer Fraud & Abuse Act (continued)	12
Copyright Act	14
Other Federal Statutes.....	16
Computer Security Act of 1987.....	20
Federal Information Security Management Act (FISMA)	21
FISMA (continued)	23
FISMA (continued)	25
FISMA (continued)	26

Fair Credit Reporting Act



- Assured access to personal information stored on computer systems
- Covers consumer credit reports
 - Prohibits obsolete information, credit bureaus responsible
 - Specifies process for consumer to obtain credit report
 - Specifies process to challenge information
- Impacts consumer privacy

304-03-12

**012 Now, we're going to go through a series of laws. It is not our intention to make you legal experts. It is our intention to make you aware of the spectrum of laws for which you are responsible. Now, let me ask you a question, you're a good military person, right? You're a system admin. Are you responsible for the law, or is that your organization's responsible for it? Can you be held personally liable for breaking the law? This is not a trick question. The answer is yes you can. Yes you can. Therefore you need to have some idea of the laws that you're responsible for, the privacy laws, and information laws, and the protections

because you are personally responsible. You cannot say I was only following orders. That won't hack it here. You are personally liable.

All right, so let's look at this. We talked about the fair credit reporting act. And it assures your access to information about you stored in computer systems. It prohibits obsolete information, credit bureau information that is their responsibility should be available to you, gives you specific process to obtain credit report, and specifies a process for you to challenge that information. And it certainly impacts your privacy.

So, you go okay so I'm a DoD sys admin, system administrator. What's that? Do you have on your system information about the people? Yes, you do. And you can, especially if you're in certain areas in financial information, have quite extensive financial information about people, or human resource information. So, therefore you need to be aware of the issues involved.

Privacy Act of 1974



- Information processed by federal agency computer systems
- Personal data to be protected
- Individual specifies what information is held, rights to obtain information held
- Physical security, management practices, and computer network controls specified
- OMB and DoD issued recent guidance concerning greater protection for Personally Identifiable Information (PII)



304-03-13

**013 All right, the privacy act of 1974, what was going on in Washington D.C. in 1974? What was special in 1974 down by the Potomac River?

Student: Watergate.

Carl Knabe: Watergate. So, what was happening in Watergate? The administration was using federal files to look up address information on potential enemies, political enemies. Not that the current people would do that, you understand. NSA would never spy on you today. Okay so, the idea was that we're going to protect the personal data. We want to keep

you the chance to challenge it. And it specified what? It's specified physical security, management practices, and computer network controls. And those specifications apply to you with your military system. That is why this is important for you to know.

In fact, Congress passed this act, was it December 31st of 1974, and was signed into law January 2nd in 1975. All right, since then the office of management and budgets, the president's office of management and budget, executive office of the president's, and department of defense have issued guidance for greater protection for personally identifiable information.

Buicks and cars, all Buicks are cars. Not all cars are Buicks. Which is more extensive, PII or privacy act? Privacy act is the bigger category. PII deals with certain things about people in that. Okay.

Counterfeit Access Device & Computer Fraud & Abuse Act - 1984



- First computer crime legislation
- Addressed unauthorized access of computer systems
 - Felony to access federal computers to obtain classified information to harm US or benefit foreign power
 - Misdemeanor to access any federal system without authorization
- Amendment in 1986 made trafficking in stolen computer passwords a criminal act

304-03-14

**014 Counterfeit access device, we looked at the phreakers, and the red box, and the ability to cracker jack whistles, and how to get into systems. This was the first computer crime legislation, computer fraud and abuse act 1984. It looked at unauthorized access of systems.

Now, look at this, it was a felony to access these federal computers to obtain classified information to harm the U.S. or benefit a foreign power. It was a misdemeanor to access the system without authorization.

Let me give you a hypothetical example. We have an ethnic Chinese-

American citizen who has a doctorate in physics. He is working in a nuclear laboratory that is in the process of constructing nuclear weapons for the United States. Okay. He's been to several conventions in mainland China. He is so dedicated to his job that he takes highly classified weapon design information, nuclear weapon design information home and puts it on his home computer so he can complete his work there. About two years later, the Chinese People's Republic turns up with identical nuclear weapons. Would you feel this individual had committed a felony or a misdemeanor?

Student: A felony.

Carl Knabe: Okay, we have some people voting for felony. Anybody for misdemeanor? Anybody for I don't know? Okay, we got some I don't know here. Okay, so what is this go to? What is the question here? The question here is, and this is where it gets very, very tricky, it goes to the intent. What was the intent of the individual? Did he, in this case he, intend to provide-- obtain customer information to benefit the People's Republic of China? Or was he simply violated-- certainly he-- this by the way, is a real case. This is not a hypothetical case. This is a real case.

Okay, so did he-- he certainly broke U.S. regulation on the handling classified data, very highly sensitive nuclear weapons design data. Okay, but did he do it to benefit them? The answer was never proven, never

proven. He did some time in jail waiting for trial, was let go. He lost his job.

The particular academic institution that was handling that lab's computer processing was replaced with another one. Okay, but when they inspected it, there were so many things wrong, hard drives behind copy processors and things. It was not a good sight. So, what you take away from this is it's very difficult here in these waters to determine what was the intent of the person when they did this.

In 1986 it was the individual arrested on the streets of San Diego selling Navy passwords. As in many cases, it became against the law after the fact.

Electronic Communications Privacy Act



- Updated Federal privacy clause in Omnibus Crime Control & Safe Streets Act of 1968
 - Legal to intercept electronic communications readily accessible to general public
 - Civil damages for illegal interception
- Unlawful access or divulgence is illegal
 - electronically stored communications
 - electronic communication service
 - remote computing service



304-03-15

**015 The electronic communications privacy act, it's legal to intercept electronic communications if they're readily accessible to the general public. If you have an illegal interception, how will you know it's illegal? Congress will pass a law and tell you. In particular, cell phone communications, it's illegal to monitor those. Federal law requires how many people be aware that a conversation's being monitored, federal law? You know when you pick up the phone to call your banking institution, and it says this conversation is being monitored for security and something? What they

really mean is to protect themselves. Okay. How many people must know that the conversation is being monitored under federal law, federal law? Just one person. Under state law like Maryland, both parties must know. So, this is to cover themselves type of thing.

Okay, where does this hit you as the DoD individual with the trust and faith of the DoD in your position as IM or assistant admin? It hits you for electronically stored communications. You have any of those in your system? Yeah. You've got a lot. Right? And electronic communication service, and remote-- got any remote computer services? Yeah, we've got those too. So, all those, this privacy act, electronic communications privacy act, applies to you. And you are subject to the provisions of it.

Computer Fraud and Abuse Act



- Signed into law in 1986; Prohibits unauthorized or fraudulent access to government computer systems.
- Maximum fine of up to \$5000 or double the value of anything obtained via the unauthorized access, plus up to 5 years imprisonment.
 - Robert Morris Jr., the author of the Internet Worm, was the first person convicted under this law



304-03-16

**016 Computer fraud and abuse act, 1986, once again fraudulent access to government computer systems, how did Congress get off? The Federal Reserve System gave them the power and authority. So, you had maximum fine of five thousand dollars or double the value. The first person was Robert Morris Jr. was the author of the first Internet worm. He was the son of Dr. Robert Morris Sr.

Now, who's heard of the Chaos club and the "Cuckoo's Egg", read the book "Cuckoo's Egg" about a KGB hacking--sponsored hacking by Chaos club, looking for Star Wars material in

the U.S. military systems? A lot of this came out of that threat. He was the son, Robert Morris Jr. was the son of the senior doctor worked for NSA and DOCKLAMP? What is DOCKLAMP? It is the unclassified name still used today by NSA for computer security information. They investigated this. I do recommend the book "Cuckoo's Egg" by Robert Morris. It was really--

Student: Cliff Stoll.

Carl Knabe: Cliff Stoll, I'm sorry.

Computer Fraud & Abuse Act (continued)



- Included in Title 18, U.S. Code
 - *Possession of Illegal Access Devices (1029)*
 - *Unauthorized Access to Govt. System (1030)*
- Crime committed when entering system to:
 - Acquire national defense information
 - Obtain financial information
 - Deny the use of the computer
 - Commit Fraud
 - Damage or deny use thru transmission of code, program, information or command
 - Further a fraud by trafficking in passwords

304-03-17

**017 Okay so, now one of the

difficulties we now have-- have you seen these widely varying numbers for how many attacks we're undergoing? Part of it is how you define an attack. Is just being pinged an attack? It can be. But do you have to actually intrude? Do you have to make it so-- how do you define when you're under attack? So, this law, this act attempted to define when a crime was being committed. If you're trying to acquire national defense information, that was a crime, get financial information, deny the use of the computer, commit fraud, damage or deny through transmission of code, and trafficking passwords once again.

Copyright Act



- Title 18 US Code, 2319
 - *Software Copyright Protection Bill*
 - Amended in Title 17 US Code, 504C & 506A
 - 10 or more illegal copies or more than \$2500—Felony!
 - Criminal penalty of Five years or \$250,000
 - Civil penalty \$100,000 per infringed work
- Software Publishers Association (SPA)

304-03-18

**018 Now, the copyright act, as was written here, was designed to protect software, sponsored by the software's publishers association. What is the digital millennium copyright act, the two thousand? That was to protect what? Movies and music, right. So, it made it illegal to traffic. Why was that more dangerous? Because with modern communications and high bandwidth, very easy for people to steal the work of artists, and movies, and music, and share them with friends. Are you responsible for that? You think you're responsible for that if somebody in your system's using peer-to-peer and sharing stuff?

Student: Yes.

Carl Knabe: Yeah, you can be a co-defendant really quickly. You are as--

I know one Army DAA that lost his position. He had a sys admin that had an OC3 and was sharing one of the early "Star Wars" movies. It was in a remote isolated position and because the way this peer-to-peer worked, it held up and said, "I'm here, I'm here and I got this bandwidth." Because it was an OC3, he crashed it.

So, the Army officer said it's a morale warfare recreation situation. We have-- we need this. We're isolated. And so, he reprimanded the system admin. They continued on. He did the same thing again. And it crashed again. This time not only was his sys admin removed, the DAA was removed. Once again consequences, we talked about consequences. Or we are talking about consequences.

Other Federal Statutes



- **Economic Espionage Act of 1996:**
 - Obtaining trade secrets to benefit a foreign entity
- **Electronic Funds Transfer Act:**
 - Covers use, transport, sale, receipt or furnishing counterfeit, altered, lost, stolen, or fraudulently obtained debit instruments in interstate or foreign commerce.
- **Child Pornography Prevention Act of 1996 (CPPA):**
 - Prohibits transmission/possession of child pornography.

304-03-19

**019 All right, there are other federal statutes that you are responsible for. The economic espionage, that's the big one we highlight-- we're highlighting to you. The electronic funds transfer act, and this is a very big thing right now with identity theft, people going and finding-- how many think it's okay to bank with your bank if you have a password and ID? Is that okay? Do it all the time, huh? How about if somebody's put-- how about if one of your children's been on the computer. And someone's got a keystroke logger? What's a keystroke logger? It logs every keystroke you make and then reports back to the

appropriate server somewhere. Okay, if it's logging every keystroke you make, it's logging your password. It's logging your ID. And it can--

I know of a case where one woman had fifty thousand dollars in a retirement account, was accessing that account, was keystroke logged. They emptied it out. And when she went to the bank, the bank said we're sorry. That was not our system that was your home system. You are responsible for that. We have no responsibility for refunding your fifty thousand dollars.

That is why in Europe, they have moved to two-factor credit cards. And they're moving in this country. The two--what's a two-factor card? Anybody here that's got a two-factor card? Yeah, you all do, hold up your CAC. That's a two-factor card. Something-- oh you don't have--

Student: Something you have in some cases.

Carl Knabe: And so, in this case, it's the ICC and the PIN number that you know.

Student: What is the two-factor?

Carl Knabe: Your password and ID don't count. Yes, I'm sorry?

Student: What is the two--?

Carl Knabe: Just a second, we need to-- yeah. Sorry, we're back into this mode now.

Student: What is the two-form factor that they're using in Europe for the credit cards?

Carl Knabe: In Europe, they have the same thing as our CAC. They have integrated circuit chip, that ICC, that little copper square. And they have the card. But so, if you go to make a purchase at the gas station or something, you put your pin in, but it has the ICC.

Now, I told you the case of my daughter who was here, national park service. And she found out her Bank of America debit card was making purchases in London. See because our cards, once you strip off-- they have the fake machines that will pick up the-- once they have that magnetic code, they're good to go. In the case of the two factor card, you have to have the ICC with the certificate in it. And you have to have the PIN number. And that's become a-- there have been some-- at least one case in the U.S. in California where a couple went and won the case against the bank, and said the bank failed to provide that, could have provided that, didn't provide that, therefore the bank was responsible for that loss.

Okay, we'll talk about this toward the end of the week, but if you want to go to jail really quickly, allow child porn to be on your system. So, if you discover child pornography on your system, what's your responsibility?

Student: Report it.

Carl Knabe: Report it to whom? The commander? Report it to who?

Student: I.G.

Carl Knabe: Report it to the I.G. That would be my number two choice. Number one choice is a criminal investigative service of some kind, OSI, NCIS, CID. Okay. Not only are you-- is that what you should do, it's what you're required to do. Can you go to the commander and say-- and the commander say that's okay I'll handle it, Martin. No. That makes him and you both-- makes you both codefendants because you're required for real, actual child pornography-- and the Supreme Court has spoken on this. We're not talking about first amendment protected pictures, odious as they may be, of children or whatever. We're talking about actual pictures of actual children, that's protected. And that's a crime.

Now, as far as naked women or naked men, that's a different issue. If they're adults-- was it Abe Ford says, the Supreme Court said, "I don't know what pornography is, but I recognize it when I see it." That is an administrative thing. We'll talk some more about this later on this week. But this certainly applies to you.

Computer Security Act of 1987



- The Computer Security Act of 1987 was signed into law in 1988
 - Prior to the enactment of FISMA in 2002, the Computer Security Act functioned as the principal information system protection policy for the federal government
- FISMA replaced the Computer Security Act as the principal information system protection policy and the requirements of the Computer Security Act have been perpetuated in FISMA and other legislation

304-03-20

**020 All right I mentioned the mother of all computer security acts. And this is reflected actually in that OMB circular A 130 appendix three I talked about. It's still there. And many of these features went into the FISMA. And FISMA stands for federal information security management act.

Federal Information Security Management Act (FISMA)



- Included as Title III, of the E-Government Act of 2002 Act, signed into law 17 December 2002
- Expounded on requirement that agencies report to Congress
- Required that agencies utilize information security best practices

304-03-21

**021 All right, FISMA was title three in the government act of 2002. And prior to that we have the GISRA, the government information security reform act I talked about. It sunsetted in November of 2002. So, in December, Congress liked it so much, and Congress was so unhappy with us and the federal government that they passed this law to keep on reporting. And I said what was the grade DoD was getting?

Student: F.

Carl Knabe: We were getting F for a long time. Then in the last couple years we've caught our way all the

way up to D plus. We have some room to go. But we have a challenge because well we have a lot of systems in DoD.

Oh, and another thing that's important, what's an-- you have an ATO, authorization to operate, right? What's an IATO?

Student: Interim.

Carl Knabe: Authorization to operate. And what does the federal government count that-- what does Congress count that? Congress counts an interim as not accredited. If it's not ATO, it's not accredited. So, you could skew your results greatly by counting all the-- because what? We favor what? When it's too hard to do, what do we tend to do? We tend to go with an IATO, right? Simple, easy. We'll just go another six months, and then we'll worry about it again sir-- okay, ma'am. So, Congress doesn't like that. They want us to stop that stuff.

And this required the agencies to utilize best security practices. Whose best security practices? Whose best security practices are required to be used for all the government agencies under FISMA? An organization called NIST, NIST, the national institute of standards and technology. Required-- before then-- before December 2002, NIST guidance was what special publications were best policy, best practices. After December 2002, they were required. There are two exemptions to that, one for the DoD,

the secretary of defense, and the other for the director of national intelligence. In both cases, it said you can have your own, recognizing that I might have more, different security concerns, you could have your own standards provided they were at least as stringent as those of the NIST. They couldn't-- you couldn't waive the NIST requirements, but you could make them more stringent. Okay.

FISMA (continued)



- Requires for both unclassified and national security programs:
 - Annual agency program reviews
 - Annual Inspector General (IG) evaluations
 - Agency reporting to OMB:
 - Results of IG evaluations for unclassified systems
 - Audits of IG evaluations for national security programs
- An annual OMB report to Congress
 - Summarizing the materials received from agencies

304-03-22

**022 All right, FISMA requires both classified and unclassified national security programs have annual reviews. For agencies that possess an IG, you're required to have the IG. If

not, you're expected to hire an independent reviewer. Okay.

Unclassified systems have the results of the evaluations, classified ones had the national security is classified. We'll talk about that in a minute.

Required audits, now what would you-- and then a summary of OMB report to Congress went to OMB, and they reported to a congressional committee on the materials received from the agencies. How do you think the DoD rates itself compared to how the DoD IG rates itself? Come on, what do you think? The IG's a lot tougher on us than we are on ourselves. So-- as they're paid to be. I guess they're motivated to be. So, that gives you an insight into the difficulty of the process.

FISMA (continued)



- Required agencies to identify risk levels associated with their systems and implement the appropriate level of protections accordingly
- Strengthened the role played by the NIST in developing and maintaining standards and guidelines for minimum information security controls

304-03-23

**023 Agencies are required under FISMA to identify risk levels. So, when you talk about the risk management framework, does it begin to make a-- we're getting a risk management framework because we're required to look at the risk levels. And you strengthen the role played by NIST in developing and maintaining standards and guidelines from minimum security controls.

FISMA (continued)



- Defined national security systems as any telecommunications or information system operated by (or for) Federal agencies which:
 - Involves intelligence activities
 - Involves cryptologic activities related to national security
 - Involves command and control of military forces
 - Involves equipment that is an integral part of a weapon or weapon system
 - Is critical to the direct fulfillment of military or intelligence missions
 - Contains information which has been specifically authorized by an Executive order or Act of Congress to be kept classified

304-03-24

**024 Now, how many of you work on a national security system? One? I see one hand, two hands, three hands, four hands, okay. How many of you work on systems that have classified information on them? Okay, guess what? You all-- all those people also-- about two thirds of the people have raised their hands. If you have classified information, you have a national security system.

Now, start off with classification of national security system started with some memorandum in the DoD. They migrated to cleaner code. And they've migrated GISRA, and now here. So, you have a national security

system if it involves intelligence activities, cryptologic activities, which is key encryption, command and control military forces. Okay, now there was an asterisk by that. And there's a little sub thing that we don't see here that says, but not-- that does not count routine administrative or financial systems. So, they assume that if your pay system goes down, the soldiers, sailors or everyone will out and mutiny and refuse to report for duty. Okay.

If it involves an integral part of a weapon or weapon systems, it is critical direct fulfillment of military operations intelligence missions. And because there was some concern that just because it was classified didn't mean it had to be, just because it didn't mean that it had to be in that security system, they said if it was specifically authorized by an executive order. And what was the executive order that told about how you classify things? What is it, one three two five six or something?

Student: Started one two five five oh.

Carl Knabe: What's--

Student: Began with one two five five--

Carl Knabe: Started with one two ninety-five. But we looked at earlier, the current one issued by the Obama administration. The point is that's an executive order. So, if your system is classified, you have a national

security system. Does that mean you have to follow national security system guidance? Yes, you do. Think about that.

For years we got by because for years they said, okay no sweat people. As long as you do the DoD certification accreditation, you're good to go. We're not going to bug you. It's changed. Now we have reciprocity, CNSSI, CNSSP policy twenty-two, which is the policy. And we have the CNSSI for the risk management.