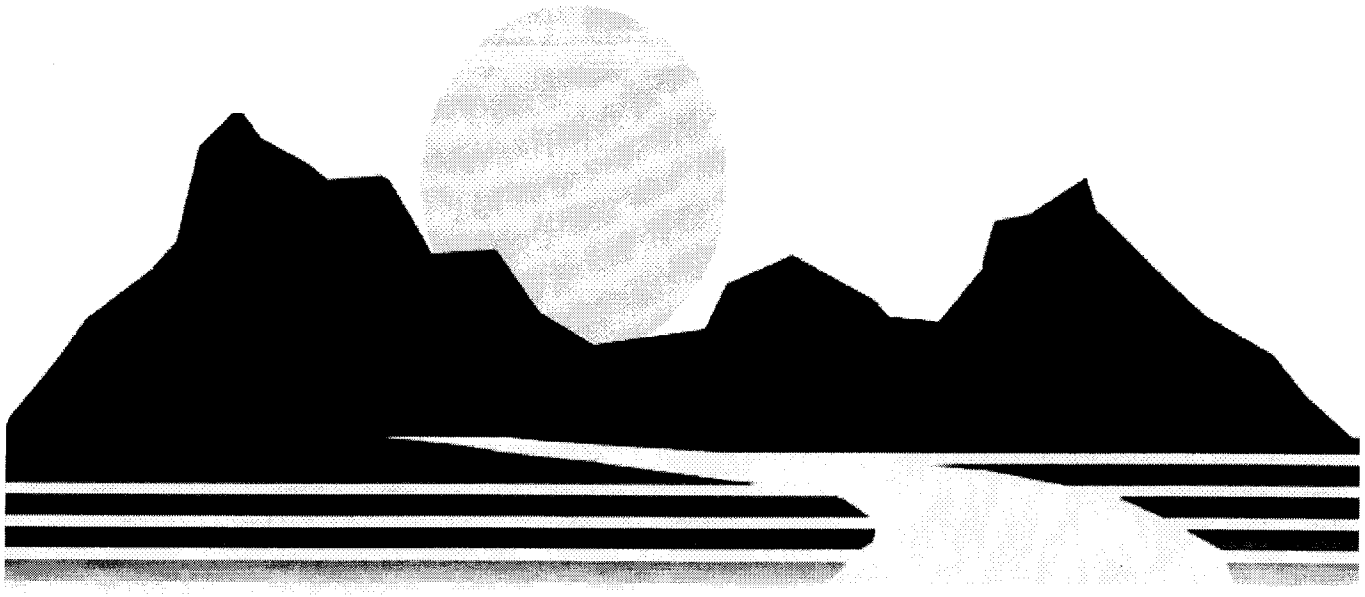


Ponemon Institute

Comments on the First Privacy Trust Survey of the U.S. Government

Dr. Larry Ponemon, Ponemon Institute
Mr. William J. Ferguson, CIO Institute, Carnegie Mellon University
Bethesda, MD. March 16, 2004

Why We Do It

Guiding Proposition 1:

- We believe that there is a strong positive correlation between the public's perception and extant practice. Those organizations with higher PTS results appear to do a superior job in managing sensitive personal information about people.

Guiding Proposition 2:

- Good privacy creates real value for organizations because it promotes the trust of key stakeholders such as employees, tax payers, customers, and organizational partners. Tangible benefits are:
  - Reduces operating bureaucracy and inefficiency
  - Improves the quality of information exchange about people
  - Decreases the risk of data security breaches and abuse

Privacy Trust Survey

- Our study is about perceptions of people concerning the privacy commitment of U.S. governmental departments, agencies and other federal organizations that are known to collect and use the public's personal information.
- Three Research Questions:
  - Do we believe that the privacy commitments of federal governmental departments, agencies and commissions vary in discernable ways?
  - Are there demographic factors that explain differences in our perceptions or beliefs about the privacy commitments of different federal organizations?
  - Do our beliefs about the importance of privacy influence what we think about the privacy commitments made by federal organizations?

Privacy Trust Defined

- Personal information – Data about yourself and your family. This information includes name, address, telephone numbers, e-mail address, Social Security number, other personal identification numbers, access codes, passwords, age, gender, income level, tax information, travel itineraries, bank account activity and many other pieces of information collected and used about you.
- Privacy commitment – Obligation of the specified government organization to keep your personal information safe and secure. This includes the commitment not to share your personal information without a just cause or without obtaining your consent to do so.

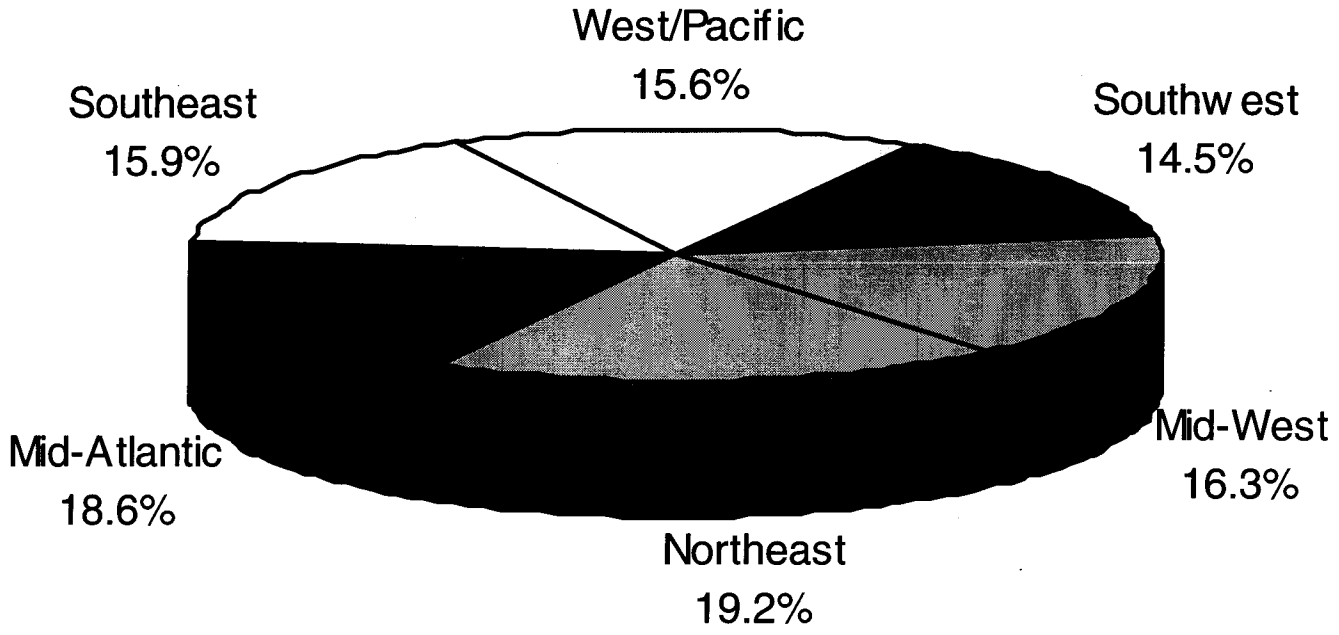
Research Process

- Expert panel: Grand list of 102 U.S. government entities that were identified as collecting and using the public's sensitive personal information (of which 53 organizations were not overlapping).
- Focus group: Grand list reduced to 60 government entities based on:
  - (1) level of privacy concern about the governmental organization's use of personal information
  - (2) belief that the organization collects and uses personal information about them or their families.
- Pilot sample: 305 adults tested survey reliability and internal validity (Web only).
- Full sample: 6,313 adults completed revised survey using three confidential channels (Web, paper and telephone).

About the Sample

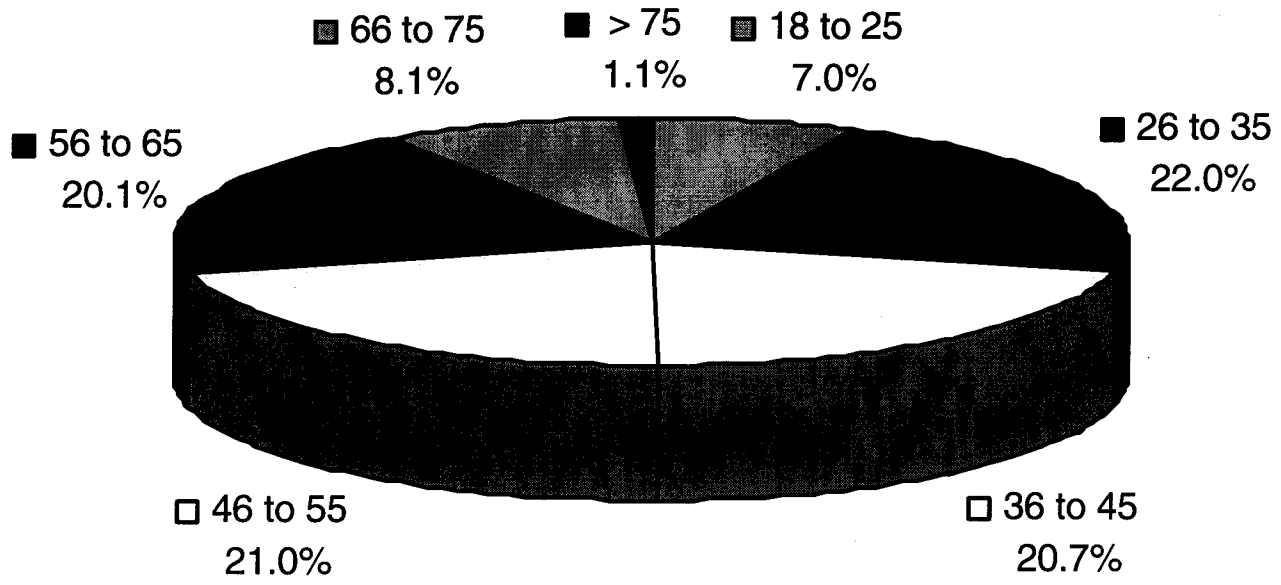
- Fixed cluster sampling frame of adults across the United States (47 states)
- Contact by paper, telephone and e-mail
  - 33,305 contacted individuals
  - 6,537 Responses to survey (20%)
  - 6,313 Usable responses (19%)
- All regions of the United States (32 States)
- Subjects compensated at $5 per completed return
- Field work completed December 19, 2003

Sample Distribution by Region



Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Sample Distribution by Age



Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

About the Survey

- Short form (about 2 printed or HTML pages) with fixed responses
- Privacy Trust is defined as:
  - Total Yes divided by Response Total
- Other measures:
  - Inverse metric = Total No divided by Response Total
  - Uncertainty metric = Total Unsure response divided by Response Total

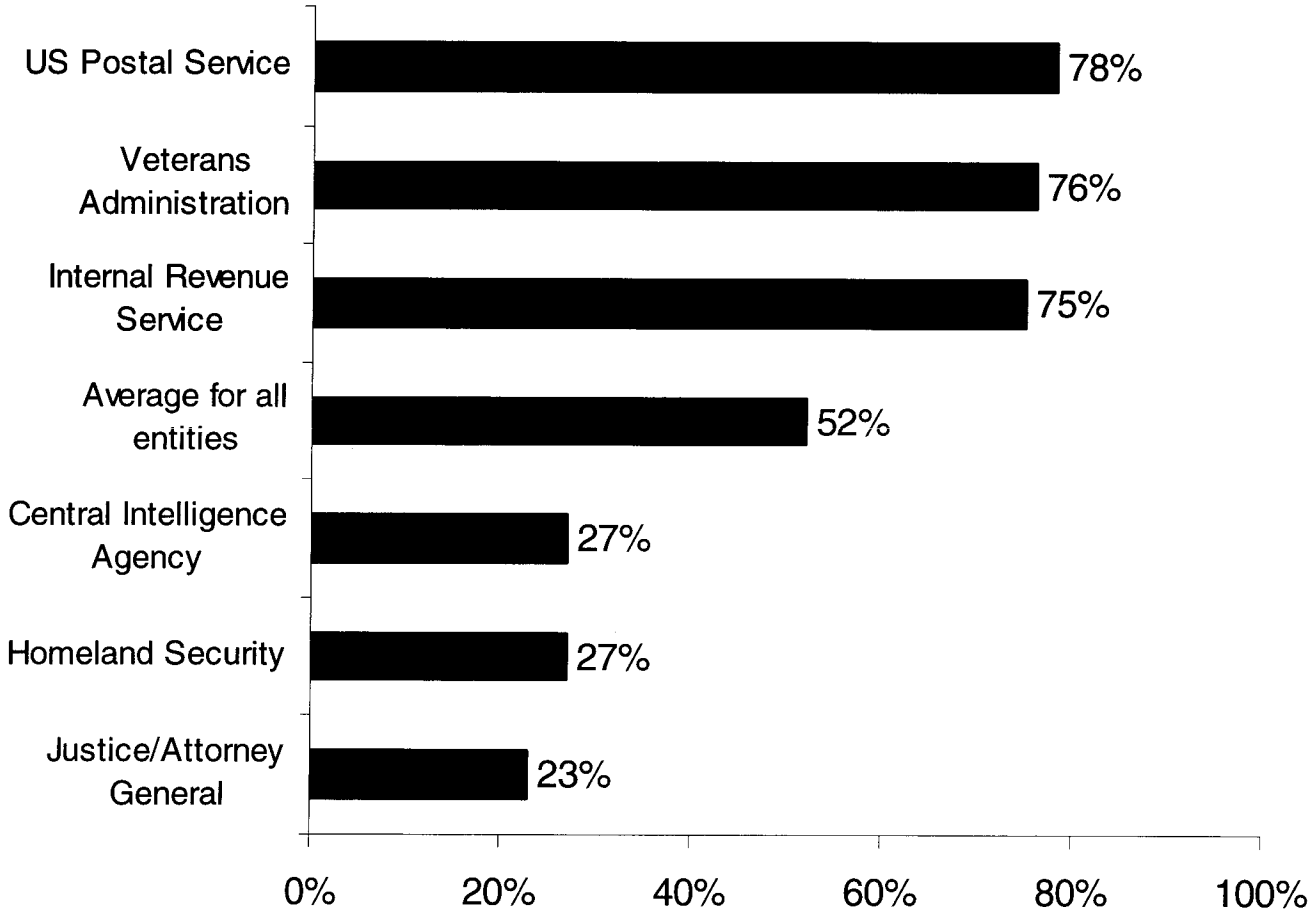
Privacy Trust Variable

- **Yes** – I feel confident that the governmental organization is committed to protecting the privacy of my personal information.
- **No** – I do not feel confident that the governmental organization is committed to protecting the privacy of my personal information.
- **Unsure** – I am not sure if the governmental organization is committed to protecting the privacy of my personal information.

Researcher Caveats

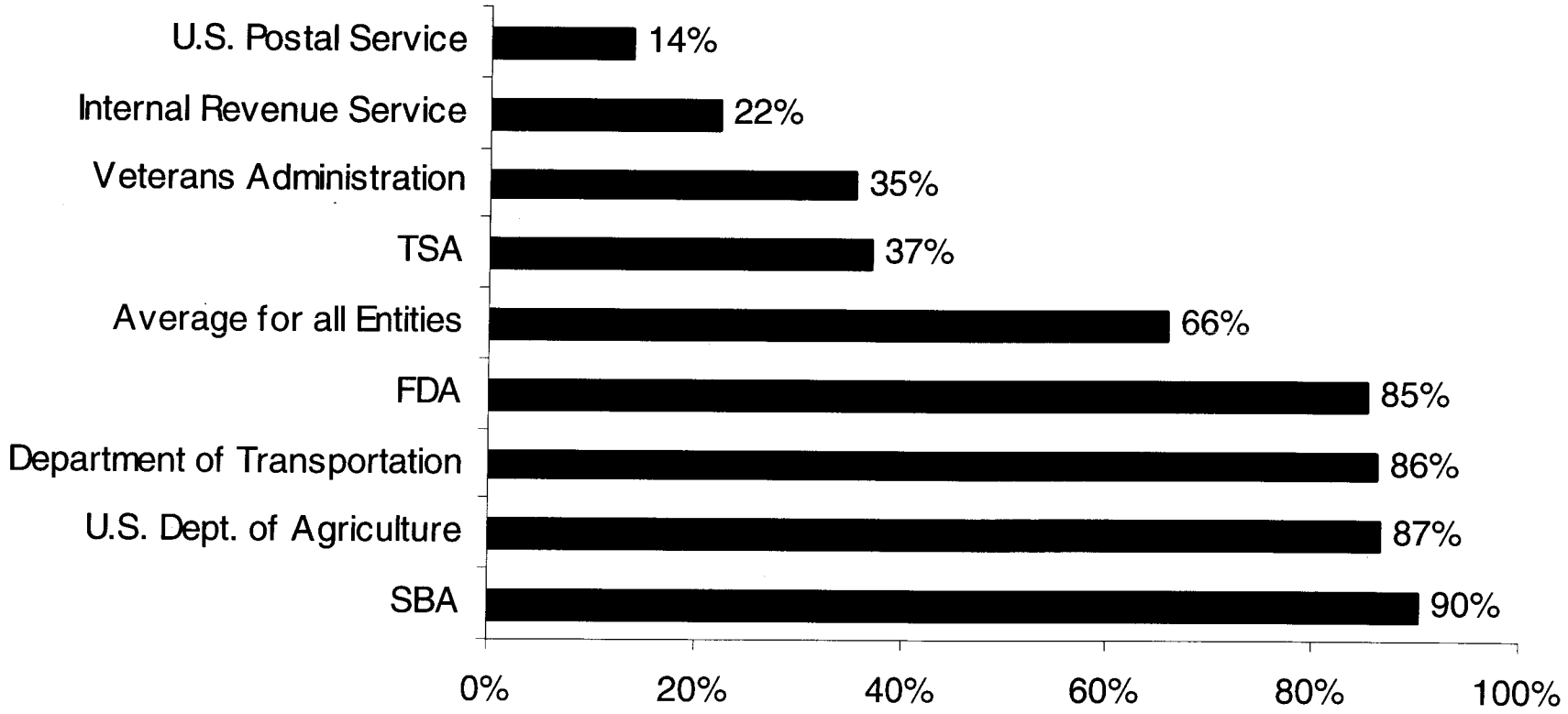
- Non-Response Bias. The current findings are based on a sample of survey returns of adults in the United States.
- Sampling-Frame Bias. The quality of results is influenced by the the degree to which the list is representative of the population of adults in the United States being studied.
- Extrapolated Behavioral Data. Analyses relies on perceptions rather than actual behaviors or firm beliefs.
- Unmeasured Variables. Other normatively important variables (such as media coverage) may have biased individual perceptions at the time of data collection.
- Self-Reported Results. The quality of survey research is based on the integrity of confidential responses received from subjects.

Government Organizations with Highest and Lowest Privacy Trust Scores



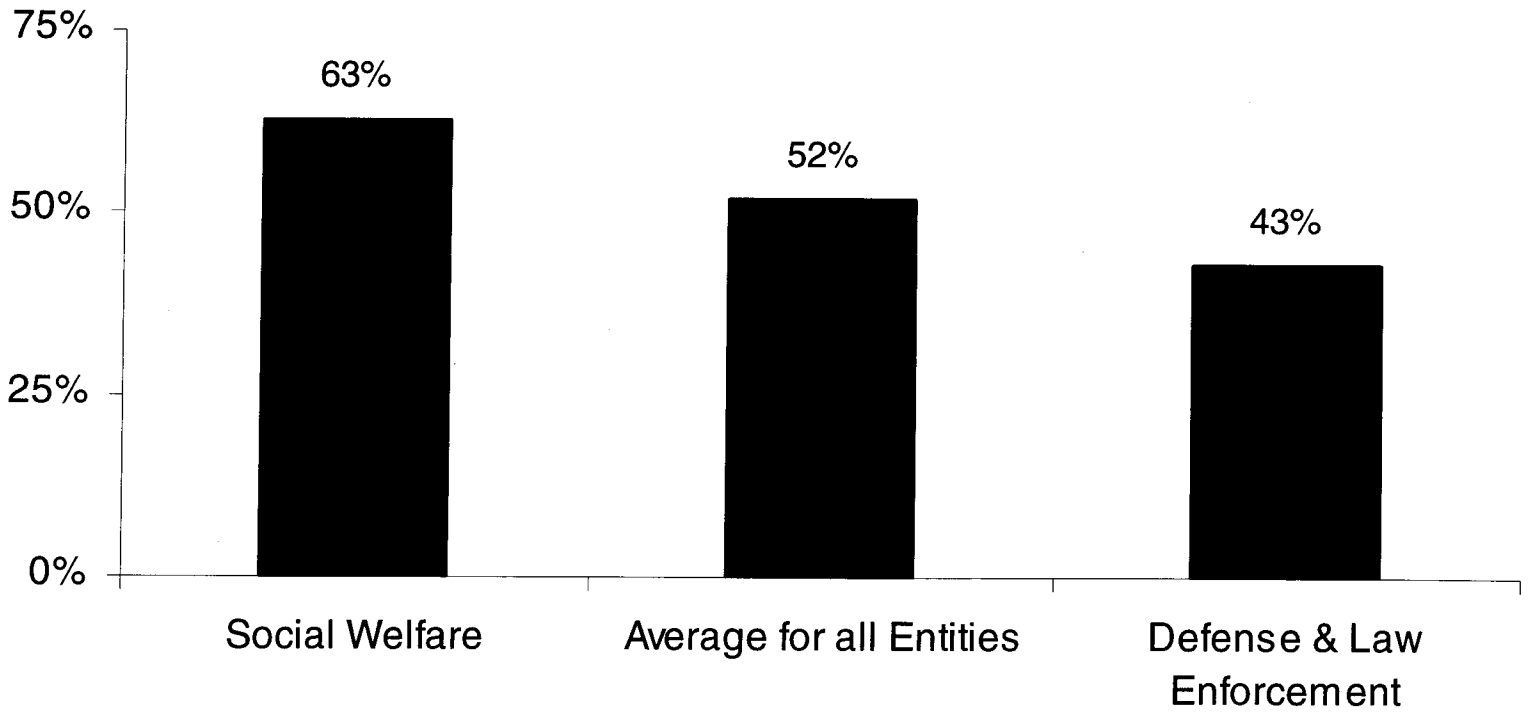
Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Government Organizations with Lowest and Highest Uncertainty Levels



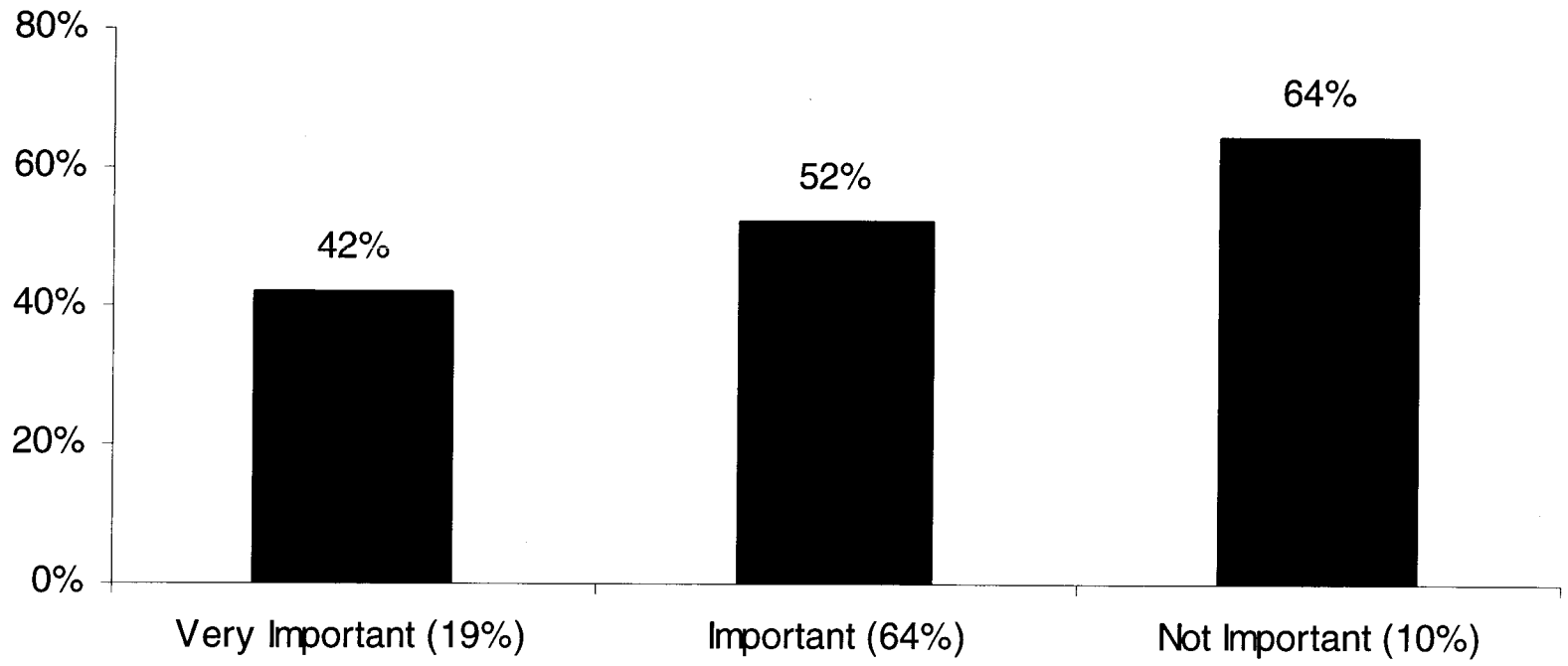
Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Entities with Social Welfare Mission versus Defense & Law Enforcement



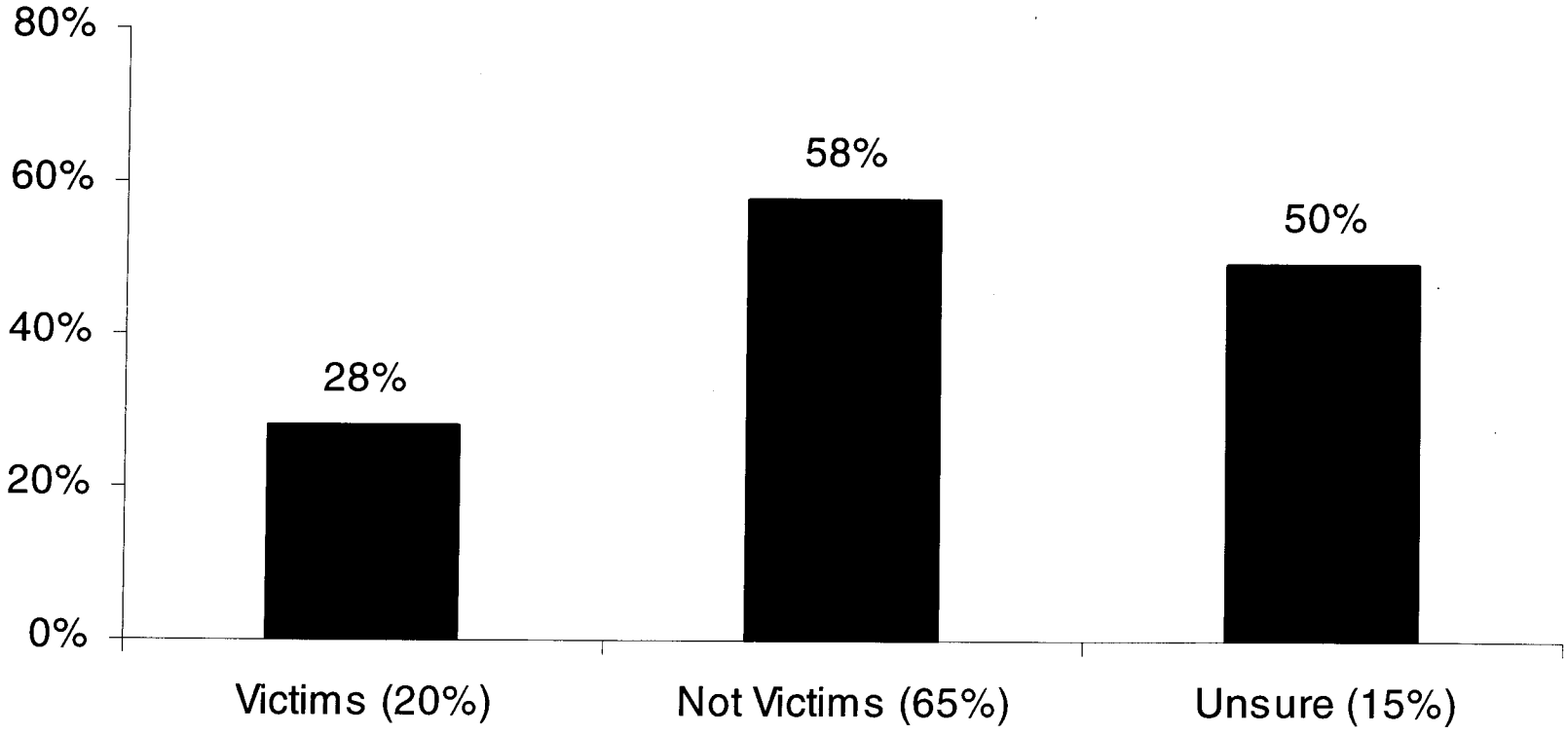
Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Average PTS by Importance of Privacy



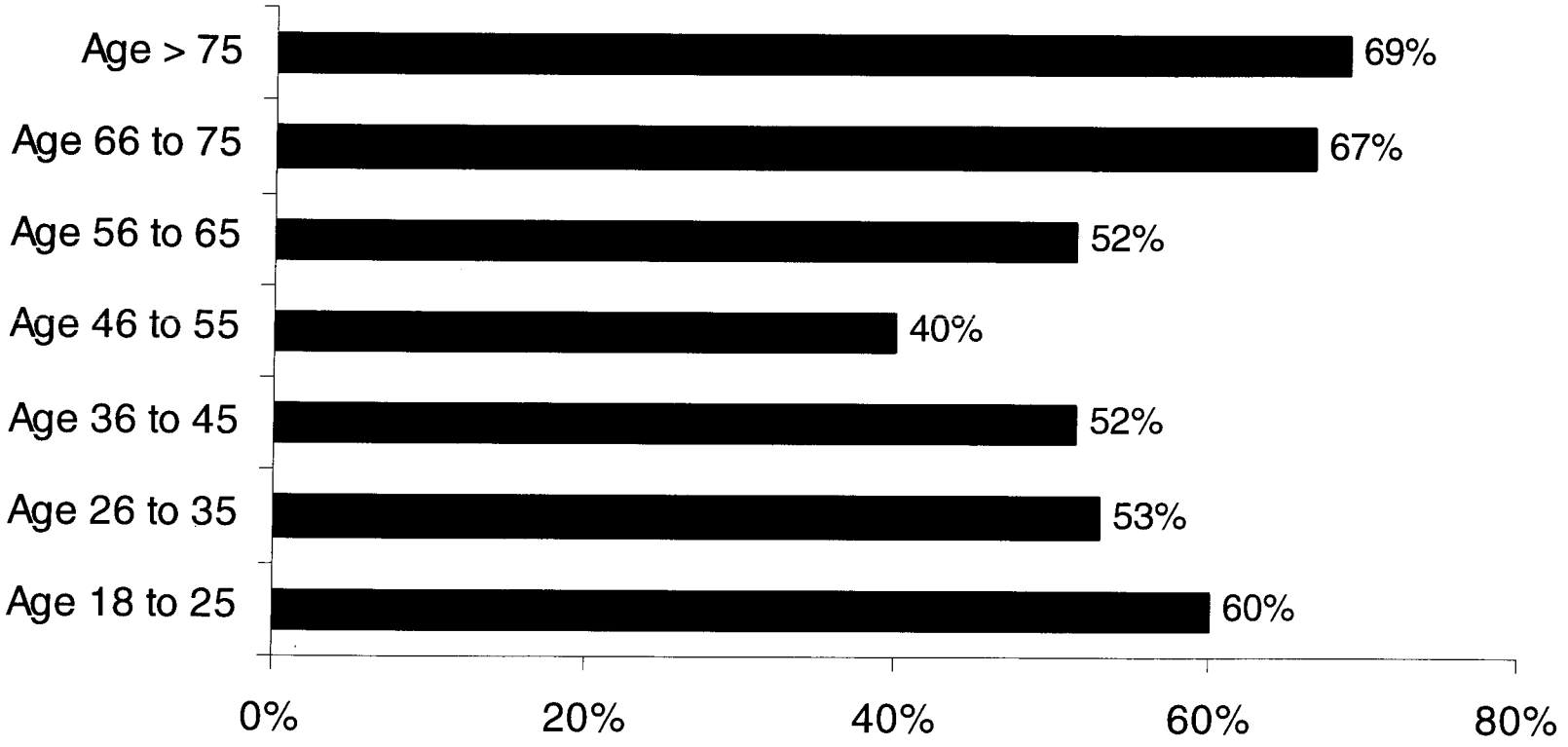
Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Average PTS by Self-Reported Rating about Being a Victim of a Privacy Abuse



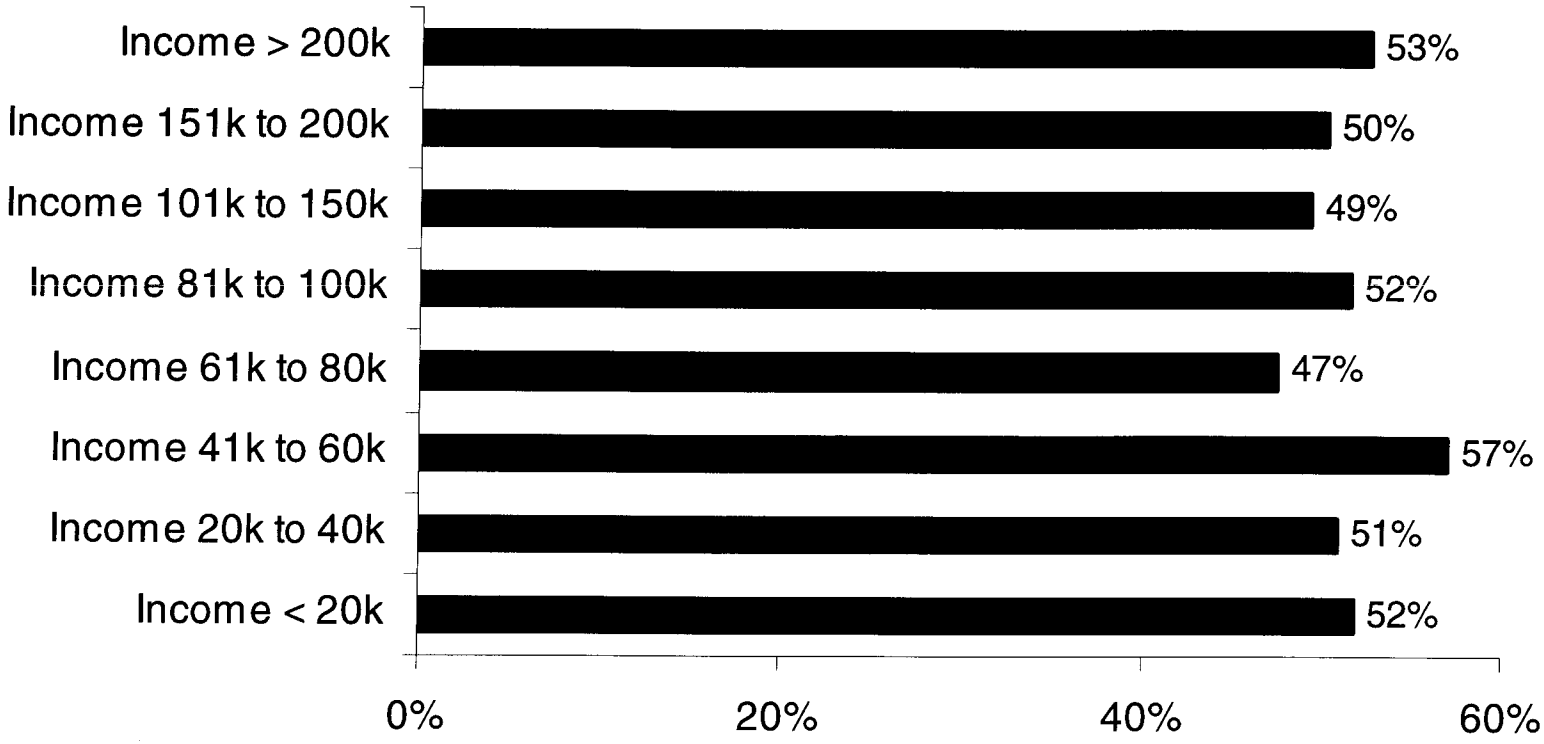
Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Average PTS by Age Range



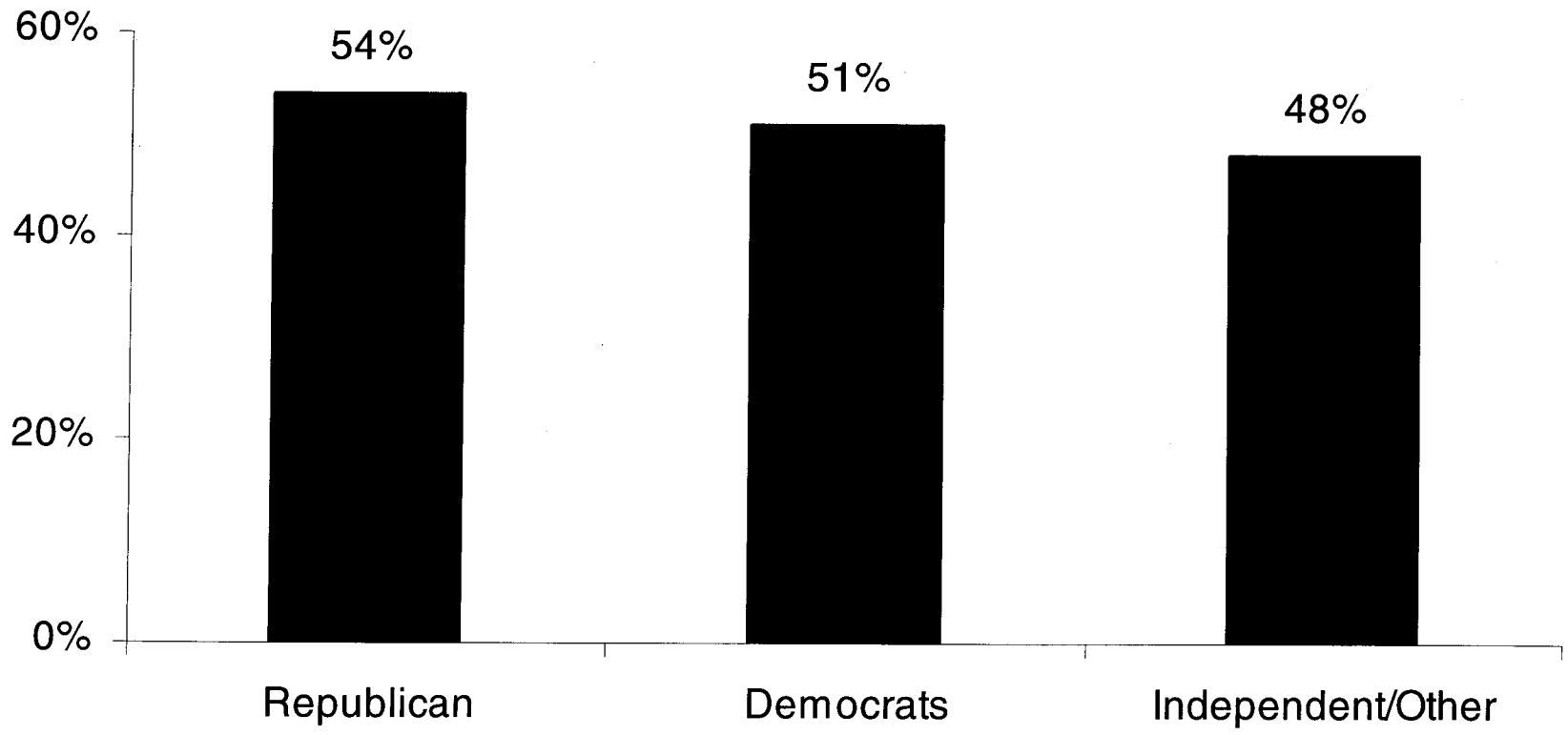
Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Average PTS by Income Range



Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Average PTS by Party Affiliation



Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

What Privacy Issues Concern Us Most?

Privacy Concerns	Total	PCT%
Theft of your identity	1,212	19%
Theft of your personal assets	1,009	16%
Sharing with state and local government	1,970	31%
Sharing with non-governmental organizations	2,146	34%
Monitoring of e-mail and Web activities	2,995	47%
Surveillance into personal life	4,001	63%
Loss of civil liberties	4,058	64%
None of the above	2,102	33%

Ponemon Institute 2004 Privacy Trust Survey ©: Based on fixed cluster sample of 6,313 adult individuals in the United States

Other Interesting Findings

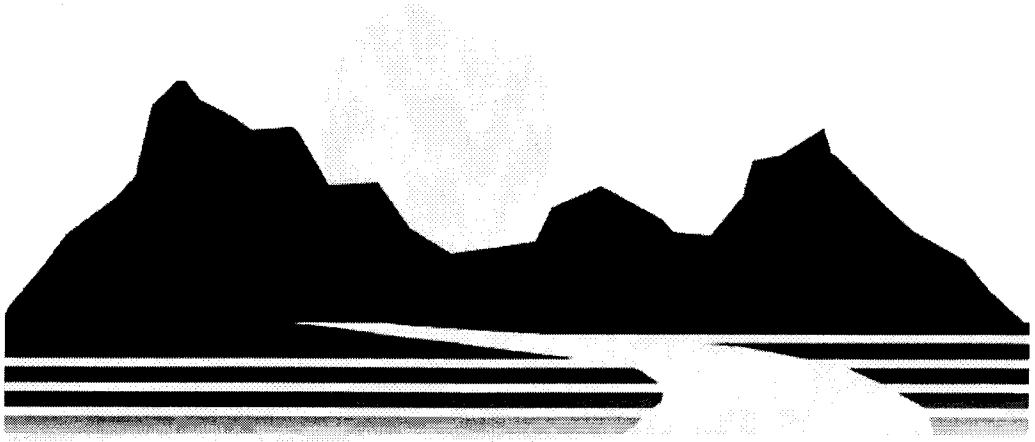
Debriefing of numerous subjects revealed the following:

- Many people do not understand the U.S. government's personal data collection and usage practices. This suggests the need for government to enhance transparency in the handling of the public's personal information. One such venue is the public disclosure of privacy impact assessments (PIAs) as required under the 2002 E-Gov Act.
- Many people have skepticism about the privacy commitments made by government, especially law enforcement and homeland security.
- Mission appears to moderate the impact of privacy. Entities that are responsible for managing criminal and terror threats against the public are given the greatest leeway for having lower privacy standards.
- Many people expressed concern that the U.S. government has lessened privacy protection to enhance its national security agenda (which sorely impacts individual freedom and civil liberties).

Questions & Answers

Dr. Larry Ponemon
Ponemon Institute
www.ponemon.org
Larry@ponemon.org
520.290.3400

Mr. William Ferguson
CIO Institute, Carnegie Mellon University
cioi.web@cmu.edu
Bferguson@cmu.edu



Ponemon Institute

Crypto and computer security in healthcare affects several areas:

1. Getting healthcare workers and organizations better trained to really achieve meaningful computer security – currently very wide spectrum in that area.
2. Encryption per HIPAA and other regs governing the protection of patient confidential information
3. E-sigs (dig sigs in particular) per 21 CFR Part 11 replacing wet sigs on e-records – which implicates a variety not only of signature-making technologies but also e-records management issues for the e-signed records; note that this may seem like a narrow topic but in fact it is an enormous one, means that clinical trials, which proceed in several phases and which today use a ton of paper and take 3-5 years to complete, may be able to be reduced to very little paper (if any) and typically 1-2 years. One example: for a major recent drug trial, of the three years it took to get FDA approval, over 50% of the time was consumed by just moving paper around for review/signoffs, especially the clinical trial results from each phase of the trials.

Four critical elements to doing all of that right:

Picking right algorithm(s)

Picking right key strengths

Getting implementation that meets appropriate standards (e.g., FIPS 140 certification/validation program)

Securing the "desktop/laptop" to ensure what is on it is what is intended – no malware

Of course, what NIST CSD does affects all four decisions

FDA/HHS regs do not yet directly prescribe FIPS compliance – hopefully that will be coming – but in the interim, there are indirect "requirements": (a) in the PKI space, for example, the Federal Bridge Certification Authority requires FIPS compliance for any CAs that cross-cert – and it is the intent of many in the private sector including pharma to cross-cert with the FBCA, which implicates compliance with FIPS; (b) several pharma companies are building or have built PKIs meeting FIPS (we did at J&J) – especially using cryptomodules meeting FIPS 140 – and aggregating into a pharma "bridge CA" emulating the FBCA; the standard for the pharma bridge are being prepared now but are expected to embed FIPS compliance; (c) beyond PKI, the standard secure configuration templates published by NSA and NIST are widely used within the pharma sector as the "gold standard" (we use them at J&J).

Let me return to the clinical trials issue for a moment, and put a fine point on that: yes, accelerating the process using FIPS crypto standards means greater profits for pharmaceutical companies because they have more time to sell their products under patent protection – but it also means saving more people's lives. The faster drugs get to market, the more patients who will benefit. So very directly, what NIST CSD does, does indeed have the real potential to save lives – and not just in a homeland security context.

Another important fact: Ex-gov folks moving to private sector which means more rapid adoption of FIPS and hence greater importance still to NIST's efforts.

So bottom line is that NIST CSD publications and work are already having a significant impact on the healthcare industry, and that impact will grow as time passes.