Comments on the First Privacy Trust Survey of the U.S. Government
Decreases the risk of data security breaches and abuse

- Improves the quality of information exchange about people
- Reduces operating bureaucracy and inefficiency

Tangible benefits are:

- Customers, and organizational partners,
- The trust of key stakeholders such as employees, tax payers,
- Good privacy creates real value for organizations because it promotes

Guiding Proposition 2:

Personal Information about people,

Higher P2S results appear to do a superior job in managing sensitive
Public's perception and external practice. Those organizations with

Guiding Proposition 1:

We believe that there is a strong positive correlation between the

Why We Do It
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?
consent to do so.

Information without a just cause or without obtaining your
This includes the commitment not to share your personal
organization to keep your personal information safe and secure.

Privacy Commitment – Obligation of the specified government

many other pieces of information collected and used about you.

tax information, travel itineraries, bank account activity and
numbert, access codes, passwords, age, gender, income level,
address, social security number, other personal identification
information includes name, address, telephone numbers, e-mail,

Personal Information – Data about yourself and your family. This

Privacy Trust Defined
Research Process

Confidential channels (Web, paper and telephone).

- Full sample: 6,913 adults completed revised survey using three validity (Web only).
- Pilot sample: 305 adults tested survey reliability and internal information about them or their families.

- (2) belief that the organization collects and uses personal organization's use of personal information
- (1) level of privacy concern about the governmental

based on:

Focus group: Grand list reduced to 60 government entities
overlapping.

Expert panel: Grand list of 102 U.S. government entities that...
Field work completed December 19, 2003

Subjects compensated at $5 per completed return

All regions of the United States (32 states)

- 6,313 usable responses (19%)
- 6,537 responses to survey (20%)
- 33,305 contacted individuals

Contact by paper, telephone and e-mail

United States (47 states)

Fixed cluster sampling frame of adults across the United States

About the Sample
Sample Distribution by Region
Sample Distribution by Age
divided by Response Total
- Uncertainty metric = Total Unsure Response
  Total
- Inverse metric = Total No divided by Response
Other measures:
- Total Yes divided by Response Total
Privacy Trust is defined as:
with fixed respondents
Short form (about 2 printed or HTML pages)

About the Survey
Privacy of my personal information.

organization is committed to protecting the

unsure – I am not sure if the governmental organization is committed to

no – I do not feel confident that the governmental organization is committed to

yes – I feel confident that the governmental organization is committed to

Privacy Trust Variable
On the integrity of confidential responses received from subjects.

Self-Reported Results. The quality of survey research is based
perceptions at the time of data collection.
(such as media coverage) may have biased individual
Unmeasured Variables. Other nonstatistically important variables
rather than actual behaviors or firm beliefs.

Extrapolated Behavioral Data. Analyses relies on perceptions
adults in the United States being studied.
the degree to which the list is representative of the population of
Sampling Bias. The quality of results is influenced by the
sample of survey returns of adults in the United States.
Non-Response Bias. The current findings are based on a

Researcher Caveats
Lowest Privacy Trust Scores
Government Organizations with Highest and

- General
- Justice/Attorney
- Homeland Security
- Agency
- Central Intelligence
- Service
- Internal Revenue
- Administration
- Veterans
- US Postal Service

- 23%
- 27%
- 27%
- 52%
- 75%
- 76%
- 78%
Highest Uncertainty Levels
Government Organizations with Lowest and

Page 13
Entities with Social Welfare Mission versus Defense & Law Enforcement

- Social Welfare: 63%
- Average for all Entities: 52%
- Defense & Law Enforcement: 43%
Average PTS by Importance of Privacy

- Not Important (10%): 64%
- Important (64%): 52%
- Very Important (19%): 42%
Average PTS by Self-Reported Rating

- Unsure (15%): 50%
- Not Victims (65%): 58%
- Victims (20%): 28%

About Being a Victim of a Privacy Abuse
Average PTS by Age Range

- Age 18 to 25: 75%
- Age 26 to 35: 69%
- Age 36 to 45: 66%
- Age 46 to 55: 66%
- Age 56 to 65: 66%
- Age 66 to 75: 66%
- Age > 75: 66%
Average PTS by Income Range
Average PTS by Party Affiliation

Independent/Other: 48%  
Democrats: 51%  
Republican: 54%
<table>
<thead>
<tr>
<th>%</th>
<th>Total</th>
<th>Privacy Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>33%</td>
<td>2,102</td>
<td>None of the above</td>
</tr>
<tr>
<td>44%</td>
<td>4,058</td>
<td>Loss of civil liberties</td>
</tr>
<tr>
<td>63%</td>
<td>4,001</td>
<td>Surveillance into personal life</td>
</tr>
<tr>
<td>47%</td>
<td>2,995</td>
<td>Monitoring of e-mail and Web activities</td>
</tr>
<tr>
<td>44%</td>
<td>2,146</td>
<td>Sharing with non-governmental organizations</td>
</tr>
<tr>
<td>31%</td>
<td>1,970</td>
<td>Sharing with state and local government</td>
</tr>
<tr>
<td>16%</td>
<td>1,009</td>
<td>Theft of your personal assets</td>
</tr>
<tr>
<td>19%</td>
<td>1,212</td>
<td>Theft of your identity</td>
</tr>
</tbody>
</table>

What Privacy Issues Concern Us Most?
which sorely impacts individual freedom and civil liberties.

Many people expressed concern that the U.S. government has lesserened privacy protection to enhance its national security agenda. Are given the greatest leeway for having lower privacy standards. Mission appears to moderate the impact of privacy. Entities that are responsible for managing criminal and terrorism threats against the public. Government, especially law enforcement and homeland security. Many people have skepticism about the privacy commitments made by assessments (PIAs) as required under the 2002 E-Gov Act. One such venue is the public disclosure of privacy impact information. One such venue is the public disclosure of privacy impact information. Many people do not understand the U.S. government’s personal data.

Other Interesting Findings
Questions & Answers
Let me turn to the clinical trials issue for a moment, and put a fine point on that: yes, "gold standard" (we use them all) --- defined standards published by NSA and NIST are widely used within the pharma sector as the expected to embed FIPS compliance (e) beyond PKA, the standard second configuration

unnoticed, the FIPS: the standard for the pharma bridge are being replaced now but are primarily used within FIPS 140-2 and reaffirming into a "bridge guard".

example: the Federal Bridge Certification Authority's requirements, particularly for any companies that have cross-over with the FCEA, which includes compliance with FIPS; (q) several pharma cross-over with the HHS in the RG & E sector, including pharma to CSAs that cross-over --- but the intent of many in the pharma sector including pharma to CSAs who cross-over --- but the intent of many in the pharma sector is clearly not for

FDAs/HHS does not yet directly prescribe FIPS compliance --- hopefully that will be an FDCA/HHS rule.

Of course, what NIST CSD does affect all four decisions

- Security the "destruction/retention" to ensure what is on it is what is included - no
- Confidentiality/Avulution program
- Compliance implementation that meets/approaches standards (e.g., FIPS 140-2)
- Protect data key security protections
- Protecting data algorithm(s)

Four critical elements to doing all of that right:

- Results from each phase of the trials
  - Informed by just moving paper around for review/selection especially the clinical trial
  - Once through all of these years 1 look to get FPA approval, over 50% of the time was
  - Result in rare, if any, and typically 1-2 years. One example: for a major
  - But in fact it is an enormous one, means that clinical trials, which process in several
  - Implications that impact not only of stringent and management of drugs but also of records
  - E.g., Site (e.g., site in particular) per 2 CFR part 11 replacing the site of records
  - 2. Encryption of HIPAA and other regulations governing the protection of patient confidential
  - Meaningful clinical security system, currently very wide-scope in that area
  - 1. Security healthcare workers and organizations better trained to really achieve

Cryptography and computer security in healthcare affects several areas:
impact on the healthcare industry, and that impact will grow as time passes.

So bottom line is that NIST CSID publications and work are already having a significant adoption of FIPS and hence greater importance still to NIST’s efforts.

Another important fact: Ex-Gov folks moving to private sector which means more rapid