Applying A Responsive Design Approach For Drafting A Pledge To Protect Information

FEDCASIC WORKSHOPS 2019

April 17, 2019 | Washington, DC

By Jacob Bournazian

Survey Statistician

Jacob.Bournazian@eia.gov

Background

- EIA has mandatory authority to collect energy information. Response rates range from 90 – 100% on most surveys

- EIA uses the Confidential Information Protection & Statistical Efficiency Act (CIPSEA) to protect 20% of the survey data collected

- Cybersecurity Enhancement Act of 2015 provides for DHS to access and monitor federal information systems; exempts DHS from liability for breaches; These provisions conflict with CIPSEA

- EIA modified its CIPSEA pledge to survey respondents to align with the Cybersecurity Enhancement Act in January 2017.

New legislation raised several issues during 2016

- How do respondents feel about the current CIPSEA pledge?
- How does changing the CIPSEA pledge impact reporting information to EIA?
- How does changing the CIPSEA pledge affect the trust relationship between EIA and its survey respondents?
- What changes to the CIPSEA pledge are needed as a result of the Cybersecurity Enhancement Act of 2015?

7 federal statistical agencies collaborated to explore these issues in 2016

Bureau of Labor Statistics	**U.S. Energy Information Administration**
Jennifer Edgar, Robin Kaplan	Jacob Bournazian
National Center for Health Statistics	**National Center for Education Statistics**
Stephanie Willson	Cleo Redline
Census Bureau	**National Agricultural Statistics Service**
Casey Eggleston, Jennifer Childs	Heather Ridolfo

Study methodology 2016

- **Cognitive interviews** (in lab & **phone**), online surveys, eye tracking

- Sample: private companies, **energy companies**, farmers, schools, household participant databases

- Cognitive interview sample size:

BLS	EIA	NASS	NCES	Total
23	25	30	24	102

Cognitive interviewing protocol

- Similar protocol cross agencies
- EIA approach:
- Read the current pledge – follow up probes
- Read two versions of the modified pledge – reversed the order for half the interviews, follow-up probes on overall impression and key concepts
  - One version mentioned Department of Homeland Security and the other version did not mention who was doing the monitoring

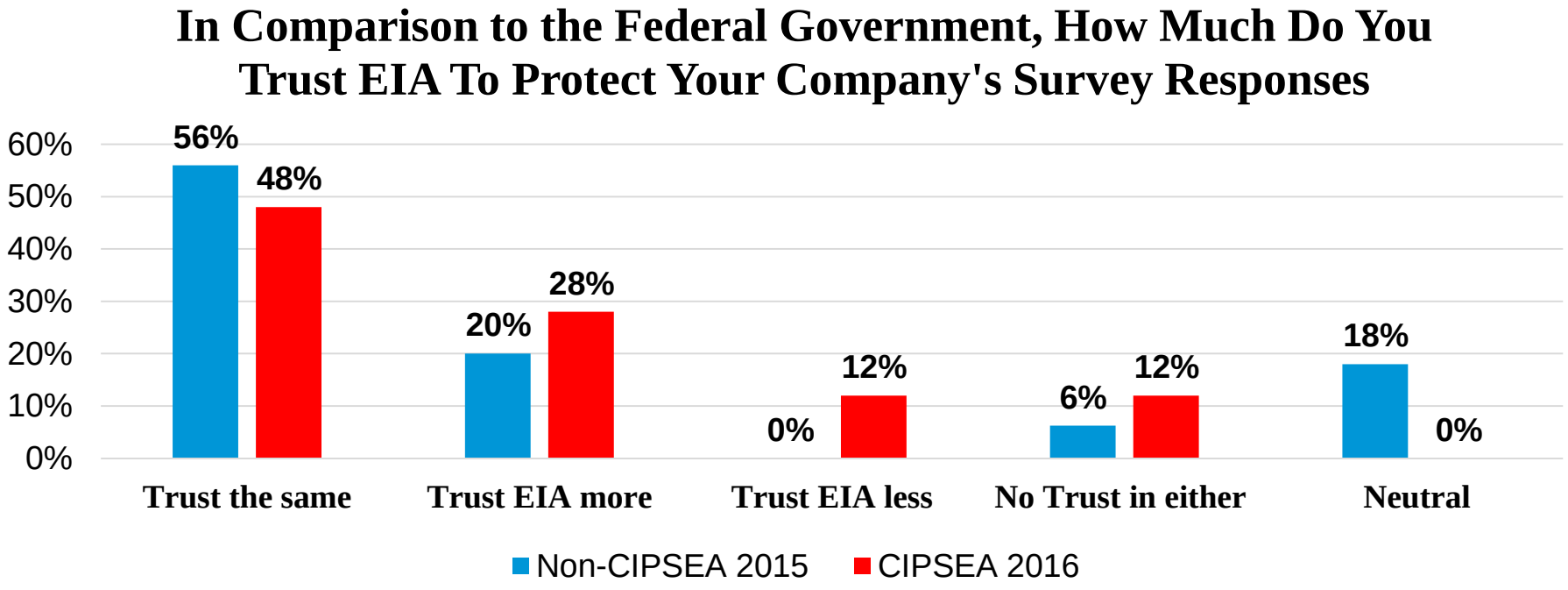
Research paper from collaborative process

Edgar, Ridolfo, Kaplan, Morrison, Willson, Redline, Eggleston, Bournazian & Hunter-Childs (2018). Proposed Model for Tailoring Confidentiality Information. Under Review *Field Methods*

- Some respondents had initial concerns after reading pledges
  - These concerns could be addressed by providing more information: Specifying who has access to their data, how it will be used, etc.
- However, some participants did not have initial concerns
  - Presenting them with more information may actually create concerns
  - Bringing up issues they hadn't thought about – other people accessing their data, etc.
- Identifying a respondent's initial reaction, survey practitioners have an opportunity to provide an appropriate response that may or may not include specific details

Results

Respondents' level of trust in EIA versus the federal government (previous study July 2015 n = 52) (July 2016 n = 25)



Data access: Testing the existing pledge used in 2016

Who can access the data you provide?	Percentage (n = 25)
EIA Staff *	96%
EIA Contractors	80%
DOE Staff	56%
Staff from other federal agencies	24%
White House Staff	21%
US Senator or Congressman	21%
IRS Staff	12%

**One respondent felt that only the survey manager could, not other EIA staff.*

Participants perception of current CIPSEA pledge - 2016

What does the pledge mean to you?	N = 25 Percentage
No public release of identifiable information	40%
Penalties apply for not protecting data	32%
No unauthorized access	20%
Statistical use only	8%

New pledge meaning - 2016

Version 1 w/o DHS	Percentage N=25
Data Security	56%
Monitoring/surveillance	28%
No unauthorized access	8%
Maintain confidentiality	4%

Version 2 w/DHS	Percentage N = 25
Explains who is doing monitoring	48%
DHS is protecting survey data	36%
EIA needs help protecting data	12%
Increased surveillance	4%

Participants perception of Department of Homeland Security

What does DHS do?	N = 22 (2016) Percentage
Protect US borders	45%
TSA airport security/protect against terrorism	28%
Security/police functions	5%
Surveillance	5%
Do not know what they do	17%

What would increase your trust in EIA's ability to protect your information?

What increases trust?	N = 25 (2016) Percentage
No action	48%
More explanation about data safeguards and penalties	40%
More competent cybersecurity staff	8%
Report less information to EIA	4%

Pathways to assess how much information to provide

Concerned Group

Path 1: Concerned → more information → assured

Path 2: Concerned → more information → not assured

Not Concerned Group

Path 3: Not concerned → more information → assured

Path 4: Not concerned → more information → not assured

Edgar, Ridolfo, Kaplan, Morrison, Willson, Redline, Eggleston, Bournazian & Hunter-Childs (2018). Proposed Model for Tailoring Confidentiality Information. Under Review *Field Methods,*

Identifying the Concerned Group - 2016

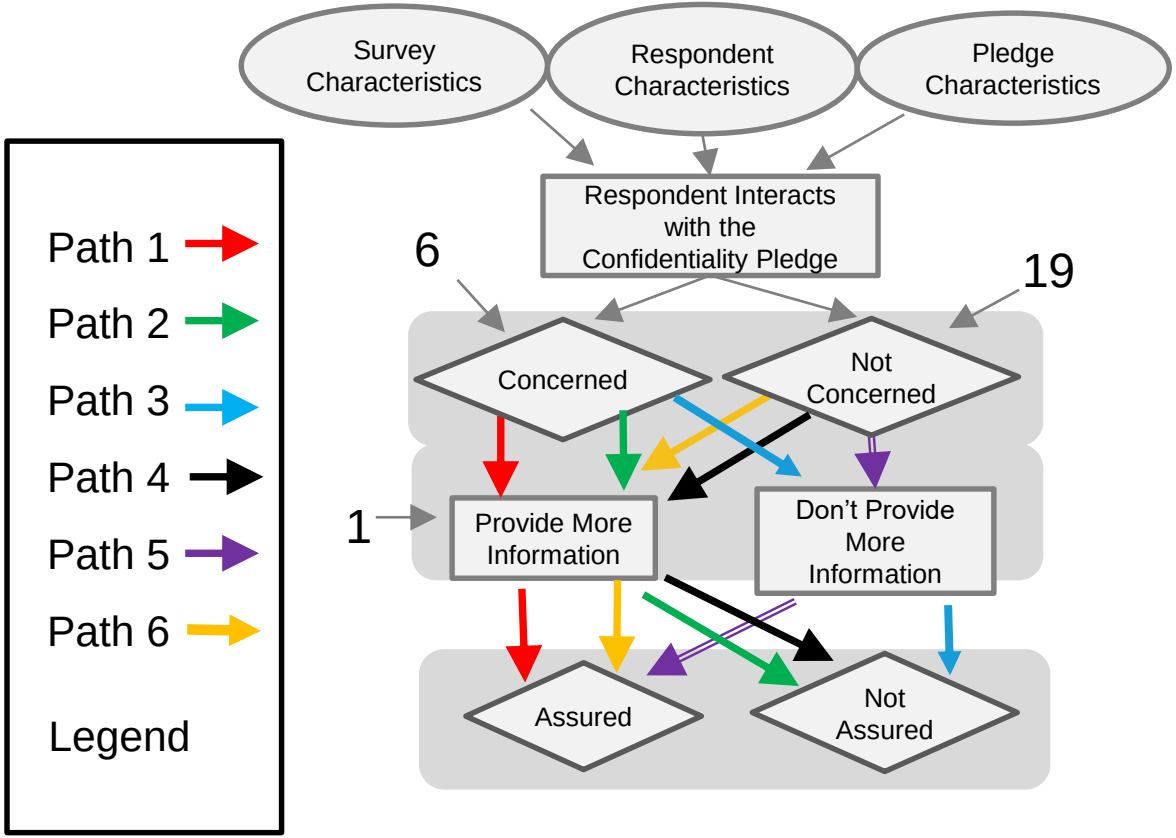
Concerned Group	EIA participants N = 6
Concerned DHS is accessing and viewing their data	2
Concerned whether DHS employees are subject to the same penalties as EIA	3
Concerned with EIA's ability to protect their data	1

Some participants wanted more information on data security
Others don't know the Department of Homeland Security

How much information and what information should be provided?

Used the version that mentions Department of Homeland Security to modify CIPSEA pledge

- Explain data safeguards and data security?
  - Do we mention monitoring and surveillance?
- Explain the activities and operations of DHS?
  - Do we mention the No Fly list and its exemption from the Privacy Act?



Pre-existing Characteristics

Introduction of Pledge

Initial Respondent Reaction

Apply Responsive Design

Final Respondent Reaction

EIA model

Benefits of using a model to draft a data protection statement

- The model discussed in the collaborative paper was not developed for this purpose, however EIA found this type of model useful for drafting privacy pledges.

- Using a model to develop a data protection statement helps maintain trust and the quality of information reported by providing pathways for adjusting to respondents reaction to information about data confidentiality policies, data safeguards, and data system security

- Improves the respondent experience by minimizing concerns over reporting information to a data collector

Future research

- Current and past research conducted at EIA regarding trust and confidentiality, suggests that using a model provides a framework for deciding what and how much information to provide in drafting a data protection statement
  - Need questions in the protocol to collect responses along the nodes in the model
- When drafting confidentiality pledge language, consider how and when additional information is presented
- There are risks associated with both presenting too little and too much information. Need to identify the reasons for concerns and the information that is useful for strengthening the trust relationship with data suppliers