infracritical

2016 ICS Cyber Security Conference, Atlanta, GA, October 24-27, 2016
Implementing a Publicly-Accessible ICS Event and Incident Database
Thursday, October 27, 2016

Bob Radvanovsky, CIFI, CISM, CIPS
rsradvan@infracritical.com

SCIDMARK

SCada Incident Database MARKup

infracritical

Reasons for SCIDMARK

- **Several reasons exist for creating database:**
  - **No such database exists that is:**
    - **Publicly available**
    - **FREE of charge (requiring ZERO payment)**
    - **Provides substantiative and attestable information**
    - **Completely "open source" (no proprietary info)**
    - **Provides useful and accessible URLs**
    - **May be utilized by several public interest groups**

infracritical

RISI Database

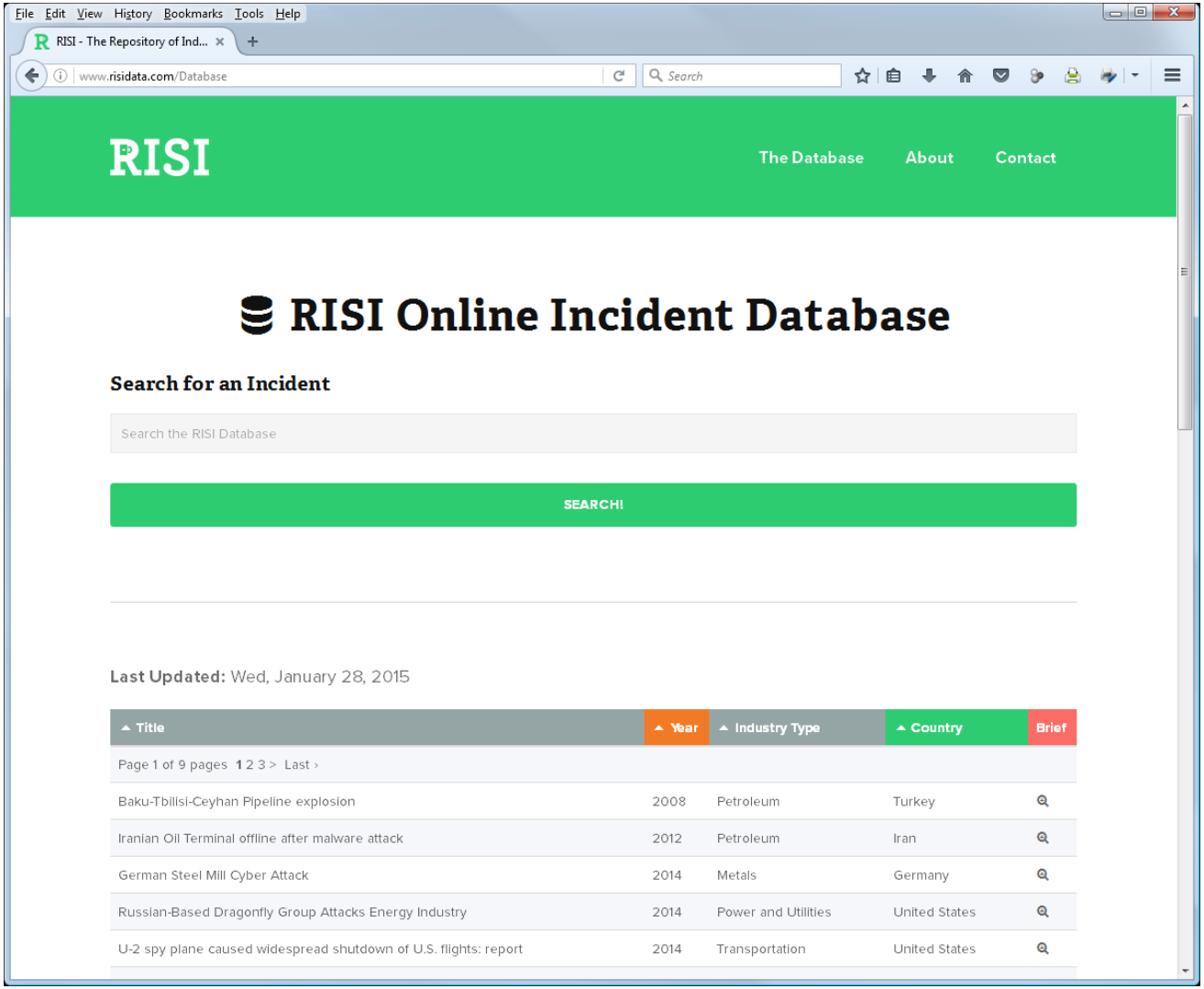
- There are a few databases, but are limited:
  - Repository of Industrial Security Incidents (RISI)
    - Formerly the “Industrial Security Incidents Database”
    - ISID incepted 2001 by Byes, Lowe and Leversage
    - ISID began at BCIT; discontinued sometime in 2006
    - Resurrected in 2008 by Byres and Fabro
    - Byres Research acquired by ‘exida’ in 2009
    - Security Incidents Organization incepted 2014

infracritical

RISI Database (continued)

The RISI database is publicly and freely available.

Web site is:
risidata.com

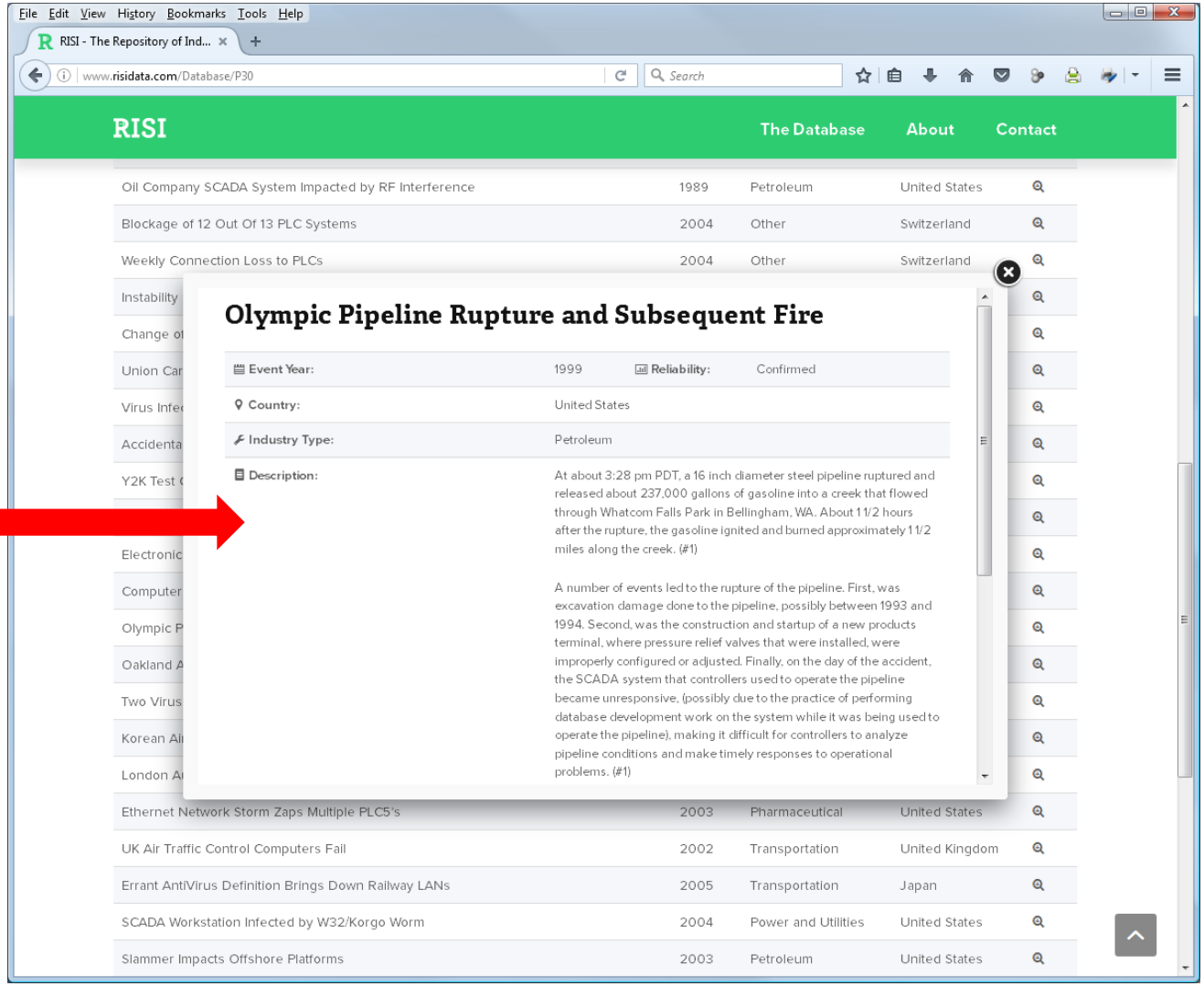


infracritical

RISI Database (continued)

This is a more detailed description of a specific incident in Olympic, WA (USA) pipeline rupture (gasoline).

3 people dead.
$45M tot. damages.



infracritical

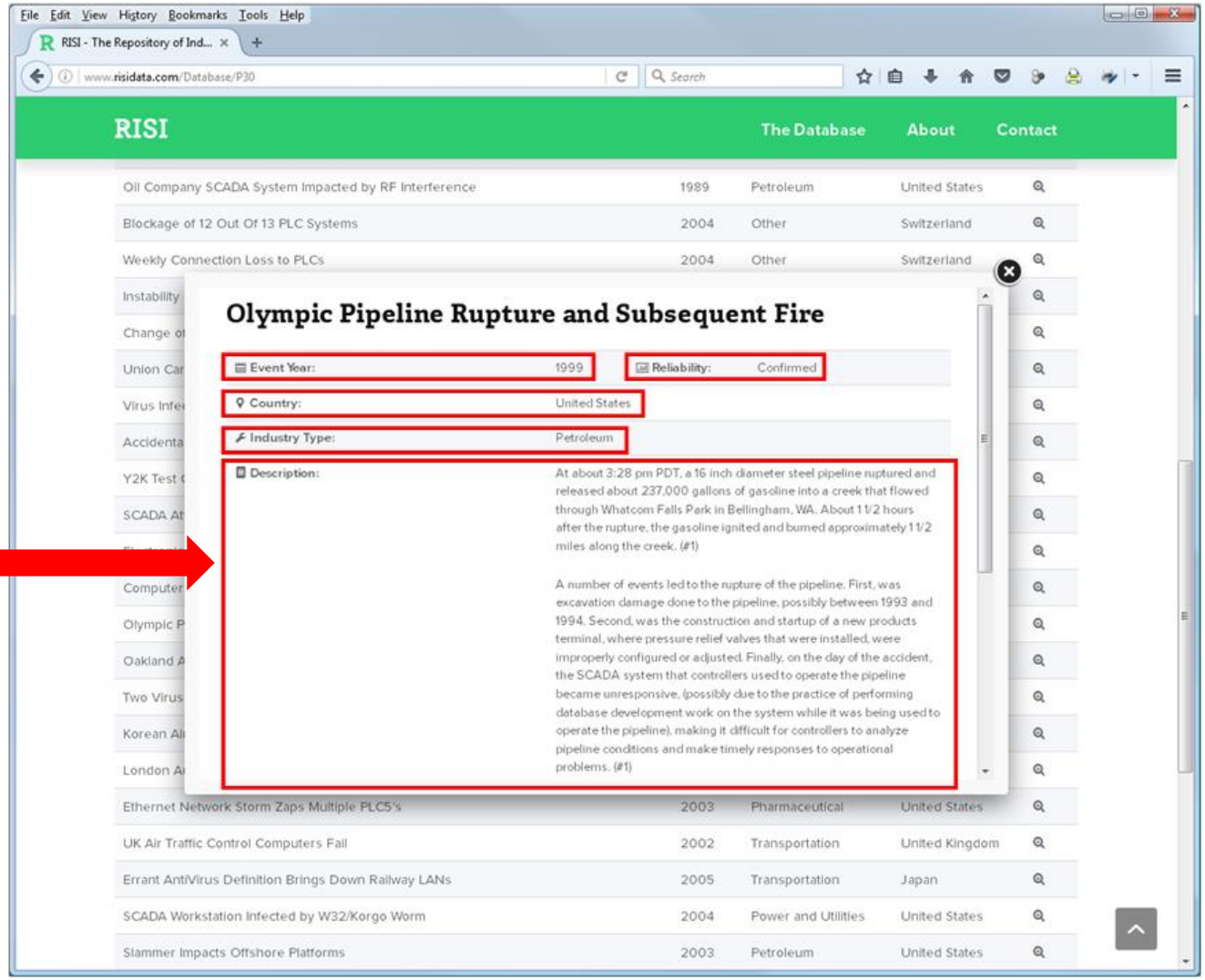
RISI Database (continued)

Only 5 significant fields identified.

Much of the detailed info is within the description field.

Could this be used for any level of attestation?

Is this substantiative?



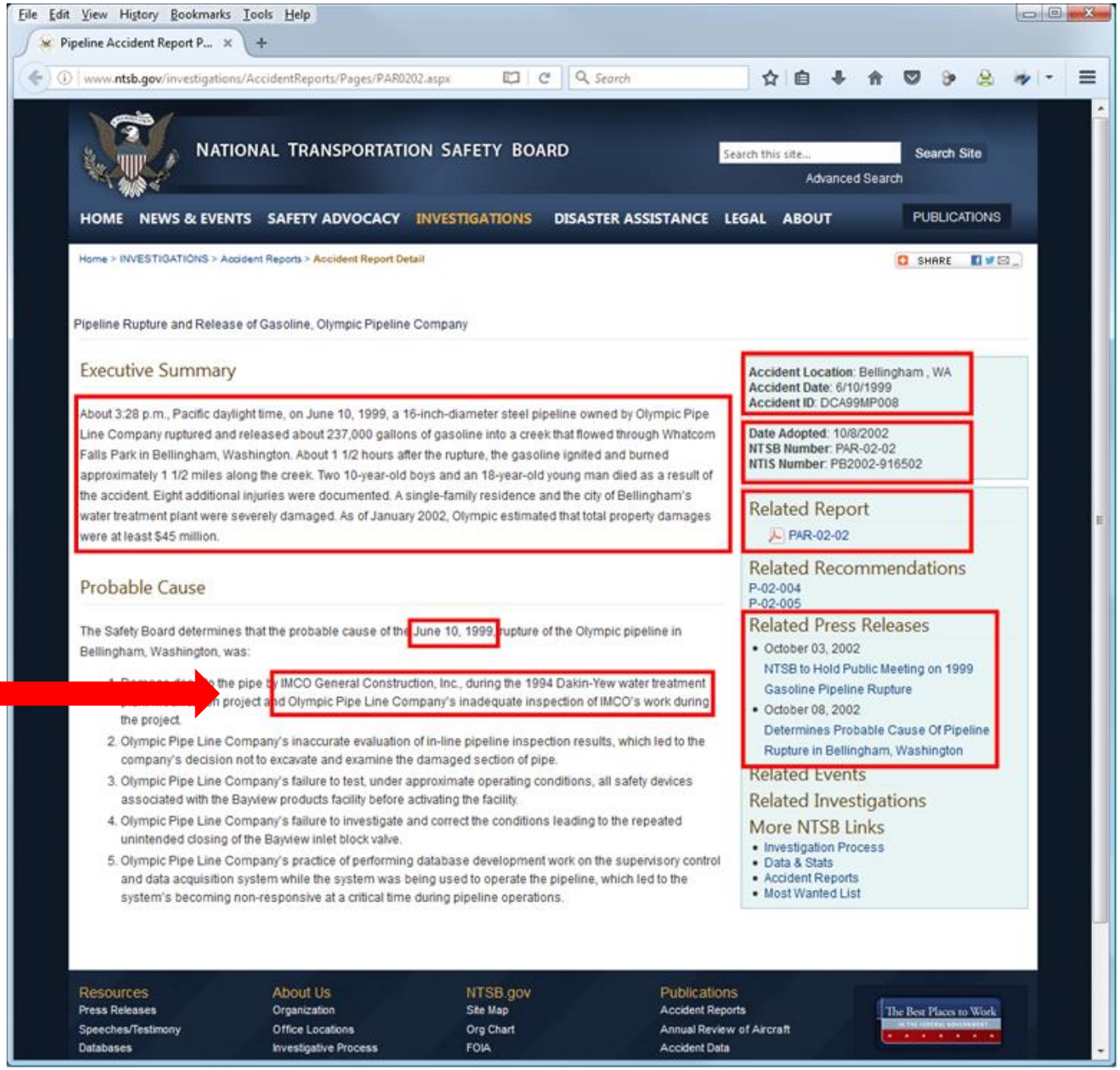
infracritical

Clearly, there are more fields identified.

More detailed info, plus source info documents for further referencing.

Could this be used for any level of attestation? **Yes.**

Substantiative? **Yes.**



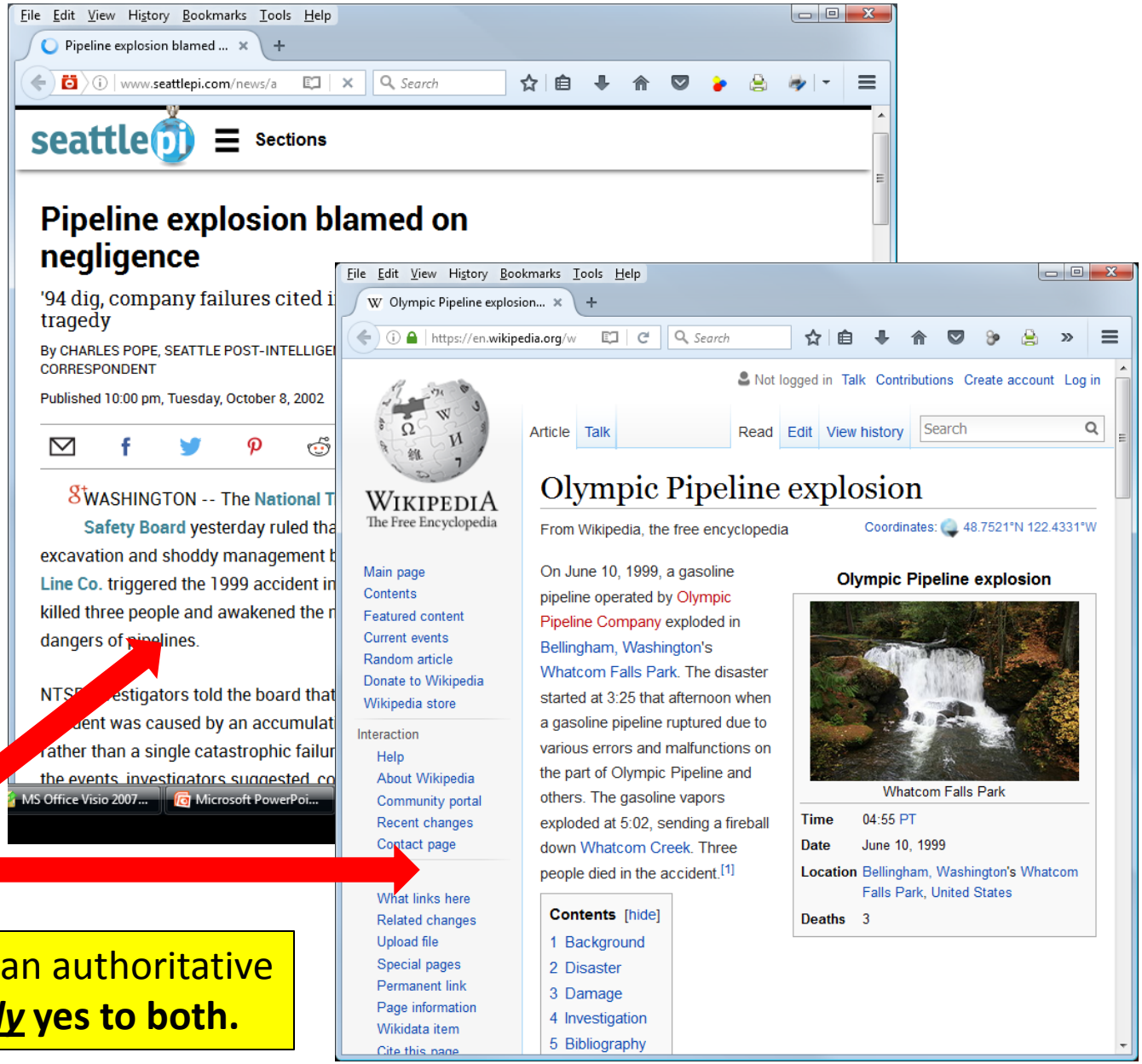
[1] http://www.ntsb.gov/investigations/AccidentReports/Pages/PAR0202.aspx

infracritical

Do these sources qualify as something reliable?

Could this be used for any level of attestation? **No.**

Substantiative? **Maybe.**



But…if combined with an authoritative source? **Then…*possibly* yes to both.**

[2] http://www.seattlepi.com/news/article/Pipeline-explosion-blamed-on-negligence-1097954.php
[3] https://en.wikipedia.org/wiki/Olympic_Pipeline_explosion

infracritical

What does this all mean?

- **What is shown is a form of intelligence…**
  - **Aggregated data, from multiple sources, that is publicly, openly, and freely available is called *"open source intelligence"***
    - **No proprietary or confidential information**
    - **No legally-privileged/restricted information**
    - **No information to compromise national security**
    - **No classified (or unverified leaked* classified) information**

* ref: Wikileaks, Public Intelligence, Pastebin, GitHub, Cryptome, et. al

infracritical

OK…so why SCIDMARK?

- **There are several benefits for this project:**
  - **Aggregated data from multiple sources…into *ONE* source**
  - **No need to search for all of the sources; most of the research is taken from as many sources as possible**
  - **Alternative sources for citing in case primary, secondary, tertiary, … et. al sources become unavailable**
  - **No need to hunt for relevant, specific information; all relevant information is broken down by 'families'**

infracritical

Uh…are there any issues?

- **There are several liabilities for this project:**
  - ***ONE*** **source can become a highly visible target**
  - **As much as having this database would benefit the 'good guys', the 'bad guys' would benefit (probably) as much**
  - **Research information at several locations by itself may prove harmless for adversaries; however, combined, this may provide a one-stop 'grocery store'**
  - **Centralized, aggregated information in one place may be considered a threat to national security**

infracritical

Are there any more concerns?

- **Perhaps…a few more:**
  - ***IF*** **such a database is considered a threat to national security, it may become a target not only by the 'bad guys', but now may become a target by the 'good guys'**
  - ***IF*** **such a database were to be contained, it could become sequestered by classifying the database itself; though this may not happen within the U.S., it may happen elsewhere…**

infracritical

Are there any negatives to this project?

- **Yes…there are a few:**
  - **Creation of such a database is entirely <u>voluntary</u>**
  - **Creation of entries within the database is manual, and would be very time consuming**
  - **Creation of relative or pertinent data may cascade into an almost endless and vicious cycle of creating more data from existing data (data of data of data…or 'metadata'); the question is 'How much is enough?'**
  - ***<u>ONE</u> <u>VERY</u> <u>BIG</u> <u>NEGATIVE</u> – the word 'cyber incident'***

infracritical

OK…so what is a ‘cyber incident’?

- ***…more to the point, how many definitions?***
  - **NIST Cyber Security Framework (CSF) does not define ‘incident’ or ‘cyber incident’:**
  - **DHS Nation Cybersecurity Incident Response Plan (NCIRP) defines ‘cyber incident’:**
    - **A cyber incident is defined as an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.**
  - **NIST SP 800-53, Rev. 4, App. B, p. B-9 (based on FIPS 200) defines an ‘incident’ as:**
    - **An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.**
  - **NIST IR 7298, Rev. 2, p. 57 defines ‘cyber incident’ as:**
    - **Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident.**

infracritical

Is there more?

- ***…oh, yes…several more…***
  - **CNSSI No. 4009 defines both 'cyber incident' and 'incident'**
    - **['cyber incident', p. 22] Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident.**
    - **['incident', p. 35] An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.**
  - **FIPS 200 defines 'incident response', but does not define the word 'incident'**
  - **NIST IR 7435 mentions 'incident', but does not define it**
  - **NIST IR 7621 mentions 'incident' and 'malicious code incident', but does not define either term**

infracritical

BUT WAIT…there's still more!

- ***…oh, yes…now onto the confusing part…***
  - **Within NIST IR 7298, Rev. 2, Glossary of Key Information Security Terms, the definition of the word 'incident' can be:**
    - **['incident', p. 90; source: NIST SP 800-61] A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.**
    - **['incident', p. 91; source FIPS 200 and NIST SP 800-53] An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.**
    - **['incident', p. 91; source CNSSI-4009] An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.**
  - **Just within this document alone, there are THREE definitions for 'incident'**
  - ***If you are part of a regulated industry, which one do you use???***

infracritical

So what can be done?

- **Right now, the U.S. federal government is focusing their efforts based on the NIST Cyber Security Framework (or "CSF") document**

- **For PCS environments, the *de facto* document of choice by regulators is NIST SP 800-53***

* **NOTE: NERC and NEI both reference and include NIST SP 800-53 as part of their cyber security controls**

infracritical

So…what's the 'big deal'?

- **Definitions are either multiple, or confusing**
  - **Definitions focus on *'information'*…instead of *'operation'***
  - **Definitions focus on the 'IT Triad':**
    - **Confidentiality, Integrity, Availability**
  - **Definitions DO NOT focus on the PCS Triad:**
    - ***Safety*, Availability, Integrity, Confidentiality**

infracritical

How would you define ‘cyber incident’?

- ***A ‘cyber incident’ is…***

“An triggered event or occurrence that either affects, disrupts, or destroys system processes responsible for, or the overall operation itself that, if executed, would impact the physical outcome of one or more functions associated to an infrastructure.”

Desktop Version

So far, it is still a proof of concept

File Edit View History Bookmarks Tools Help

Small Business - Start Bootstra...

Search

About Services Contact

Occurrence Information

LOSS OF TELEMETRY W/PUMP [UNIT 41A]

SCIID# 2014091401
ENTITY: FIRST ENTERGY CORPORATION

SEVERITY: CRITICAL COUNTRY: US

SECTOR: HEALTHCARE/PUBLIC HEALTH
SUBSECTR: ENERGY//DISTRIBUTION

Press LINK for more detailed information.

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

Detec

DL: E DT: M DPT: A
MTD: LE LEM: IDS DER: E

DDAT: 08/25/2016 DTIM: 1425C ** DETECTION
RDAT: 08/29/2016 RTIM: 1425C ** RESPONSE
RESP: 36 DAYS ** RESP IN

DETECTION INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

Damage Information

OC: Y DAM: Y RCV: Y

DAMAGE INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

DAMAGE $: $1M
RECVR $: $10M
RECVR TIME: 6 MONTHS

ADDITIONAL INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

Web Information

TOP 5 URL LINKS

L-01: CNN: Finding issues with industrial controls directly connected to the Internet

L-02: NBC: Is there really a problemi with directly connecting devices to the Internet?

L-03: CNN: Problem with the Internet

L-04: CNN: Problem with the Internet

L-05: CNN: Problem with the Internet

Penetration Information

PT: E PE: CE POE: L POET: H

PENETRATION INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

Regulatory Information

RV: Y RFK: N

REGULATORY INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

REGULATR: NERC COUNTRY: US
STATUTE: NERC CIP R6.3, S1.3.4
STATUTE: NERC CIP R6.3, S1.3.4
STATUTE: NERC CIP R6.3, S1.3.4
FINE $: $10M
FINE DATE: 02/01/2018

Impact Information

OIS: P OIT: LOT ODS: TEMP CAUSE:
ENV: D ECO: P HUM: NON INCORRECT TELEMETRY

DESCRIPTION HERE -- Lorem ipsum dolor sit amet, consectetur adipisicing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

ODAT: 08/25/2016 OTIM: 1425C ** OCCURRENCE
RDAT: 08/29/2016 RTIM: 1425C ** RECOVERY
EDAT: 08/29/2016 ETIM: 1230C ** ENTRY TO DB

RECOVERY DESCRIPTION --

Attack Information

ATK: Y AT: C AM: SABO AV:

ATTACK INFO HERE -- Lorem ipsum dolor sit elit. Saepe rem nisi accusamus error velit anir Recusandae, suscipit, soluta quibusdam accus eveniet eligendi dolor consectetur. sdkfjshfdks ofsdofdis wiousdhsd sihhf iewsu si i siufdsh isd sisudy is ydisdu fgsigfivsb isisdu ssiusdhydfis si sisdi ysdidyfi sisisi fyh sisisisug y is ifu sisgisyfis hsisisihhs ihgfis. sdfyuo vw o sdio vos osd oi d goibudf odf odfiudf dobgi dudodi fdb ddodifd odfodfoi ddfo fdh di dodfo ugdo gfuo djj.

Legal Information

CV: Y FIN: Y

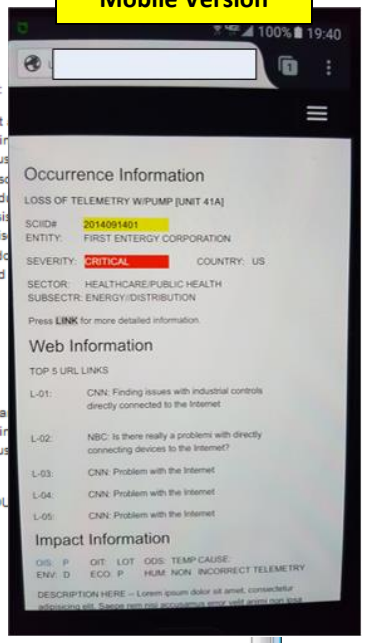
LEGAL INFO HERE -- Lorem ipsum dolor sit a elit. Saepe rem nisi accusamus error velit anir Recusandae, suscipit, soluta quibusdam accus eveniet eligendi dolor consectetur.

LAW ENFR: FBI COU

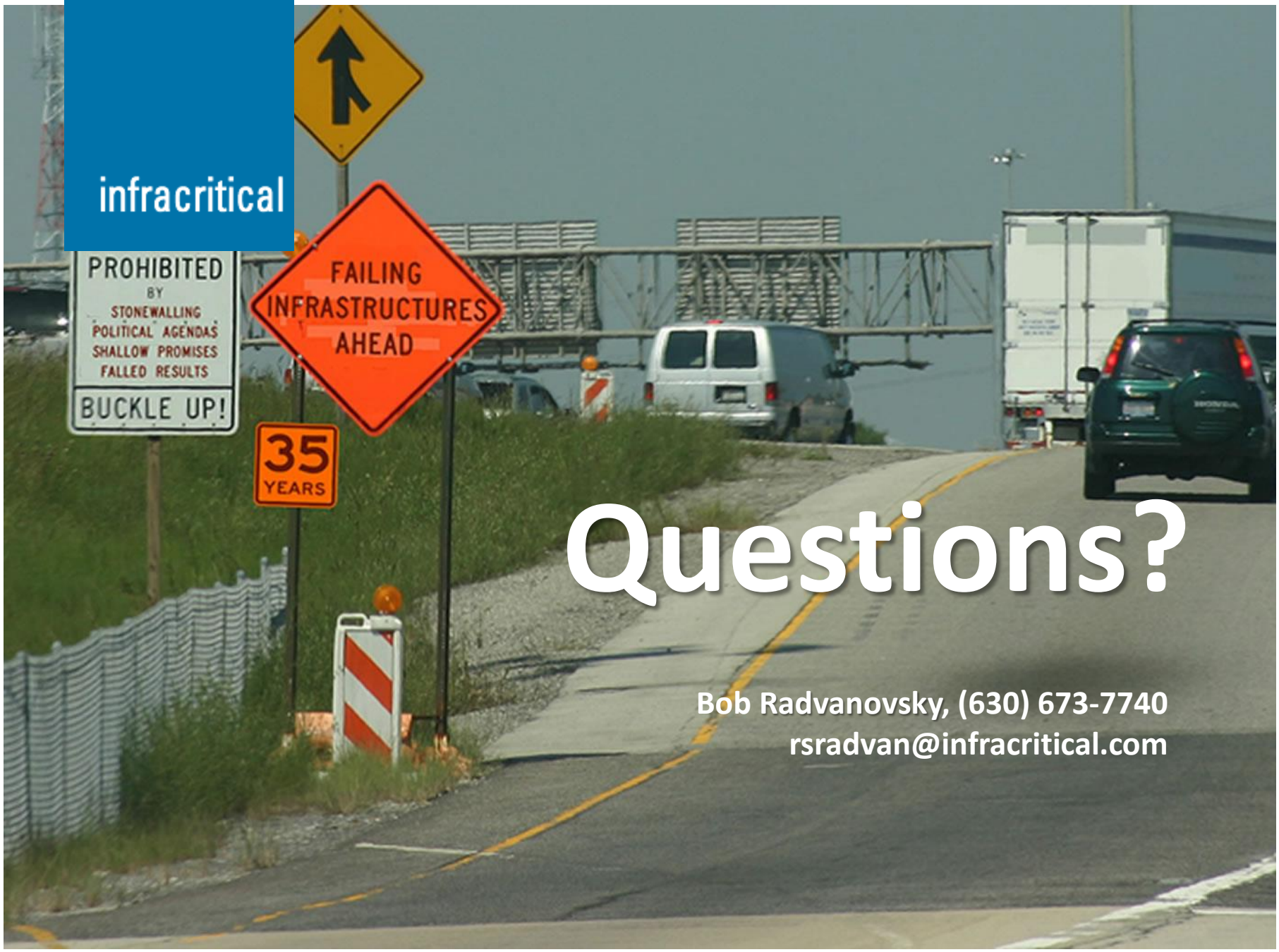
STATUTE: 18 USC 1060 (B)(9)(a)
FINE $: $100,000
FINE DATE: 02/01/2018
ARST DATE: 02/01/2018
HEAR DATE: 02/01/2018
SENT DATE: 02/01/2018
IMPR DATE: 02/01/2018

Copyright © Infraeritical. All rights reserved.

Mobile Version



SCIDMARK uses Twitter's Bootstrap v3; works seamlessly on any device


infracritical
PROHIBITED
BY
STONEWALLING
POLITICAL AGENDAS
SHALLOW PROMISES
FALLED RESULTS
BUCKLE UP!
FAILING
INFRASTRUCTURES
AHEAD
35
YEARS
Questions?
Bob Radvanovsky, (630) 673-7740
rsradvan@infracritical.com