

Date: 12/13/2005

Attn: PPAU, UC

Squad Oakland RA

Contact: SA

Drafted By:

Case ID #: 314-SF-124261 (Pending) - 255
 ✓ 800A-SF-136730 LIA (Pending) - 81

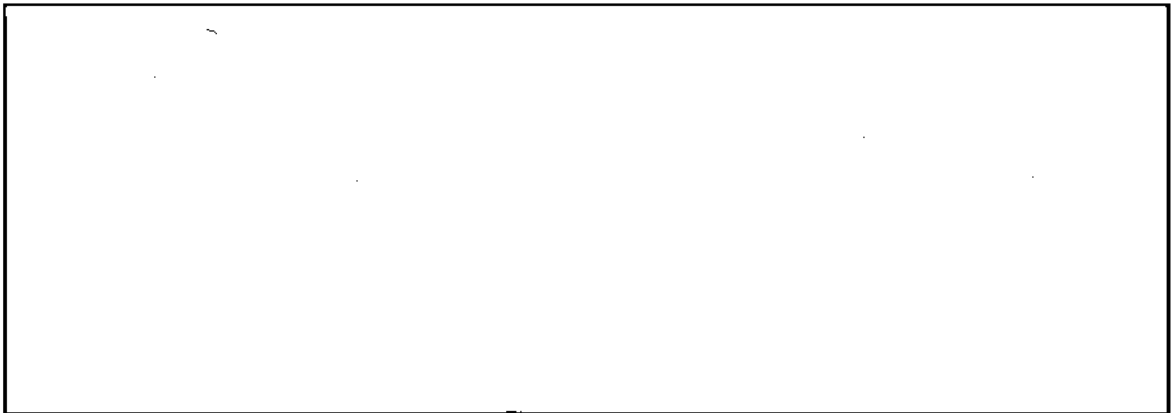
Synopsis: To document telephone conversation with

Enclosure(s): Copy of EC, by SA [REDACTED] dated 10/03/2005
which describes [REDACTED]

believes that InfraGard

in Sacramento. He further stated that the FBI has no credibility after the events of 9/11.

To: Cyber From: San Francisco
Re: 314-SF-124261, 12/13/2005



b6
b7C
b7E

[redacted] concluded the hour-long conversation by generously offering to speak at an SF Bay InfraGard meeting. The writer intends to follow up on this offer.

For the benefit of the reader, the following information is provided as a supplement to [redacted] comments:

The National Infrastructure Security Co-ordination Centre can be found at www.niscc.gov.uk. The site is divided into three sections: information; products and advice; and information sharing. Under the information sharing section is [redacted]: Information Exchanges. According to the website, Information Exchanges are based upon the personal trust of the representatives who share information in a confidential setting. Trust is built up slowly. Representatives are expected to attend all meetings which are held every two months. Each organization can have two representatives and cannot send substitutes. The NISCC has a specific Information Exchange for SCADA and Control Systems Information Exchange. Additional information is also available on ICS with documents describing best practices for Process Control and SCADA Security, Firewall Deployment for SCADA and Process Control Networks as well as bulletins on Hackers Targeting utilities control systems and warnings about terrorists' interest in water supply and SCADA systems. It should be noted that the NISCC has no regulatory, legislative or law enforcement role.

b6
b7C
b7E

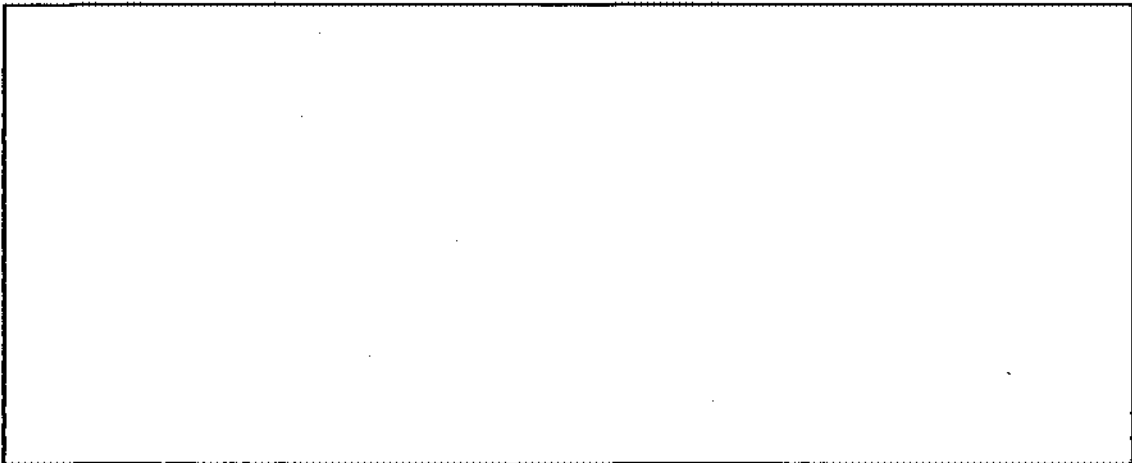
[redacted] has testified before Congress numerous times. On [redacted] testified before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. During this testimony [redacted] emphasized that control systems are different from traditional IT systems and that these systems are not secure because there is inadequate information sharing and technology. While much attention has been paid to

To: Cyber From: San Francisco
Re: 314-SF-124261, 12/13/2005

securing IT systems, virtually nothing has been done to secure ICS. Additional vulnerabilities include the following:

- There are a limited number of suppliers of process control systems in the world therefore the same systems are sold in virtually every country throughout the world.
- Control systems are designed to be efficient, not secure.
- Business and economic forces have pressured companies to interconnect their business network with their control systems which exposes the ICS to the multitude of threats from the Internet.
- Process control systems are not replaced with the rapidity of IT systems. Only when a ICS becomes obsolete does it get replaced hence adding security is a long term project.

concluded his testimony by stating that eCERT (a CERT designed to meet the needs of ICS) and the National SCADA Test Bed can help strengthen the security of the control systems.



b6
b7C
b7E

♦♦