



Repository for Industrial Security Incidents  
(RISI Incident Submission Form V7)

Today's Date				<b>Tick right hand box to keep information confidential</b>
<b>Your Contact Information</b>				
(All reported incidents will be confirmed, and as such you will be contacted. You affiliation with the reporting will be permanently removed following this confirmation.)				
Name				
Title				
Company				
E-mail				
Phone number				
RISI Investigator				For RISI Use Only
RISI Entry Date	Year:	Month:	Day:	
Investigator Comments				
<b>General Information</b>				
Title of Incident				
Reliability				For RISI Use Only
Date of Event	Year:	Month:	Day:	<input type="checkbox"/>
Name Of Company/ Organization Impacted				<input type="checkbox"/>
Location of Incident	City: _____			<input type="checkbox"/>
	State/Prov: _____			<input type="checkbox"/>
	Country: _____			<input type="checkbox"/>
Industry Type	<input type="checkbox"/> Aerospace <input type="checkbox"/> Petroleum <input type="checkbox"/> Automotive <input type="checkbox"/> Pharmaceutical <input type="checkbox"/> Chemical <input type="checkbox"/> Power and Utilities <input type="checkbox"/> Electronic Manufacturing <input type="checkbox"/> Pulp and Paper <input type="checkbox"/> Food & Beverage <input type="checkbox"/> Telecommunications <input type="checkbox"/> General Manufacturing <input type="checkbox"/> Transportation <input type="checkbox"/> Metals <input type="checkbox"/> Unknown <input type="checkbox"/> Mining <input type="checkbox"/> Water/Waste Water <input type="checkbox"/> Other _____			

<b>Incident Details</b>		
Incident Type	<input type="checkbox"/> Accidental Equipment Failure <input type="checkbox"/> Accidental Inappropriate Control <input type="checkbox"/> Accidental Incident <input type="checkbox"/> Accidental Network Failure <input type="checkbox"/> Accidental Software Failure <input type="checkbox"/> Audit <input type="checkbox"/> External- Denial of Service (DoS) <input type="checkbox"/> External- Fraud <input type="checkbox"/> External- Information Theft  <input type="checkbox"/> Other _____ <input type="checkbox"/> Unknown	<input type="checkbox"/> External- Sabotage <input type="checkbox"/> External- System Penetration <input type="checkbox"/> External- Virus/Trojan/Worm <input type="checkbox"/> External Incident <input type="checkbox"/> Internal- Insider Fraud <input type="checkbox"/> Internal- Non-Authorized Access <input type="checkbox"/> Internal- Sabotage <input type="checkbox"/> Internal Incident
Perpetrator	<input type="checkbox"/> External <input type="checkbox"/> External- Activists <input type="checkbox"/> External- Agencies of Foreign States <input type="checkbox"/> External- Competitor <input type="checkbox"/> External- Hacker/Virus Writer <input type="checkbox"/> External- Script Kiddies <input type="checkbox"/> External- Terrorist  <input type="checkbox"/> Other _____	<input type="checkbox"/> Insider <input type="checkbox"/> Insider- Current Contractor <input type="checkbox"/> Insider- Current Employee <input type="checkbox"/> Insider- Former Contractor <input type="checkbox"/> Insider- Former Employee <input type="checkbox"/> None <input type="checkbox"/> Unknown
Point of Entry	<input type="checkbox"/> Local- Business Network <input type="checkbox"/> Local- Communications Channel Media <input type="checkbox"/> Local- Human Machine Interface (HMI) <input type="checkbox"/> Local- Laptop <input type="checkbox"/> Local- Physical Access to Equipment <input type="checkbox"/> Local- Programming Terminal <input type="checkbox"/> Local Access <input type="checkbox"/> None <input type="checkbox"/> Physical	<input type="checkbox"/> Remote- Corporate WAN <input type="checkbox"/> Remote- Dial-up Modem <input type="checkbox"/> Remote- Internet Directly <input type="checkbox"/> Remote- SCADA Network <input type="checkbox"/> Remote- Telco Network <input type="checkbox"/> Remote- Trusted 3 <sup>rd</sup> Party Connection <input type="checkbox"/> Remote- Via Business Network <input type="checkbox"/> Remote- VPN Connection <input type="checkbox"/> Remote- Wireless System <input type="checkbox"/> Remote Access <input type="checkbox"/> Unknown <input type="checkbox"/> Other _____

<p>How was security problem detected?</p>	<input type="checkbox"/> Internal Staff <input type="checkbox"/> Security Device/ Log Alert During Incident <input type="checkbox"/> Contractor During Incident <input type="checkbox"/> Contractor After Incident <input type="checkbox"/> Security Consultant/ Investigator <input type="checkbox"/> Internal Cntrl/ Op Staff During Incident <input type="checkbox"/> Internal Cntrl/ Op Staff After Incident <input type="checkbox"/> Internal IT Staff During Incident	<input type="checkbox"/> Internal IT Staff After Incident <input type="checkbox"/> Security Device/ Log Alert <input type="checkbox"/> Security Device/ Log Alert After Incident <input type="checkbox"/> Found During Routine Audit Activity <input type="checkbox"/> Reported by Outside Agency/ Non-Employee <input type="checkbox"/> Unknown <input type="checkbox"/> Other _____	
<p>What Security was in Place Prior to the Incident?</p>	<input type="checkbox"/> 802.1X <input type="checkbox"/> Access Control <input type="checkbox"/> Biometrics <input type="checkbox"/> Detection Systems <input type="checkbox"/> Digital Certificates <input type="checkbox"/> Digital ID's <input type="checkbox"/> Encrypted Files <input type="checkbox"/> Encryption <input type="checkbox"/> Firewall- Dedicated <input type="checkbox"/> Firewall- Host Based <input type="checkbox"/> Firewall- Router Based	<input type="checkbox"/> Firewall- VLAN <input type="checkbox"/> Firewalls <input type="checkbox"/> In-Line Encryption Devices <input type="checkbox"/> Intrusion Detection System <input type="checkbox"/> None <input type="checkbox"/> Password Access Control <input type="checkbox"/> PKI Encryption <input type="checkbox"/> Unknown <input type="checkbox"/> Virus Protection Software <input type="checkbox"/> VPN <input type="checkbox"/> Other _____	
<p>Remedial Action Taken</p>	<input type="checkbox"/> Technology- Installed Router or VLAN <input type="checkbox"/> Hardware <input type="checkbox"/> Hardware- Replaced <input type="checkbox"/> Hardware- Upgraded <input type="checkbox"/> Procedural - Upgraded Patching Procedures, Unknown <input type="checkbox"/> None <input type="checkbox"/> Software- Patched <input type="checkbox"/> Technology - Installed Intrusion Detection System, Unknown <input type="checkbox"/> Software Upgraded <input type="checkbox"/> Technology- Installed Firewall <input type="checkbox"/> Procedural- Changed Password	<input type="checkbox"/> Unknown <input type="checkbox"/> Software <input type="checkbox"/> Technology- Changed Firewall <input type="checkbox"/> Procedural <input type="checkbox"/> Security Technology <input type="checkbox"/> Procedural- Changed Access Procedures <input type="checkbox"/> Procedural- Changed Audit Procedures <input type="checkbox"/> Technology- Deployed Encryption/VPN <input type="checkbox"/> Procedural- Changed Equipment Use Rules <input type="checkbox"/> Technology- Installed AntiVirus System <input type="checkbox"/> Other _____	

<p>Attempted Result of Incident</p>	<input type="checkbox"/> Environmental Spill <input type="checkbox"/> Equipment Damage or Loss <input type="checkbox"/> Fine/ Penalty <input type="checkbox"/> Fraud <input type="checkbox"/> Illicit Use of Equipment <input type="checkbox"/> Injury or Death <input type="checkbox"/> Intellectual Property Theft <input type="checkbox"/> Loss of Communications <input type="checkbox"/> Loss of Data <input type="checkbox"/> Loss of Equipment Control	<input type="checkbox"/> Loss of Production/Operation <input type="checkbox"/> Loss of Staff Time <input type="checkbox"/> Loss of View <input type="checkbox"/> Loss/ Contamination of Product <input type="checkbox"/> None <input type="checkbox"/> Public Nuisance/Inconvenience <input type="checkbox"/> Public Injury or Death <input type="checkbox"/> Unknown <input type="checkbox"/> Other _____	
<p>Achieved Result of Incident</p>	<input type="checkbox"/> Environmental Spill <input type="checkbox"/> Equipment Damage or Loss <input type="checkbox"/> Fine/ Penalty <input type="checkbox"/> Fraud <input type="checkbox"/> Illicit Use of Equipment <input type="checkbox"/> Injury or Death <input type="checkbox"/> Intellectual Property Theft <input type="checkbox"/> Loss of Communications <input type="checkbox"/> Loss of Data <input type="checkbox"/> Loss of Equipment Control	<input type="checkbox"/> Loss of Production/Operation <input type="checkbox"/> Loss of Staff Time <input type="checkbox"/> Loss of View <input type="checkbox"/> Loss/ Contamination of Product <input type="checkbox"/> None <input type="checkbox"/> Public Nuisance/Inconvenience <input type="checkbox"/> Public Injury or Death <input type="checkbox"/> Unknown <input type="checkbox"/> Other _____	
<p>Approximate Financial Impact</p>	<input type="checkbox"/> \$0 <input type="checkbox"/> <\$10,000 <input type="checkbox"/> \$10,000 - 100,000 <input type="checkbox"/> \$100,000 - \$1,000,000	<input type="checkbox"/> \$1,000,000 - \$10,000,000 <input type="checkbox"/> >\$10,000,000 <input type="checkbox"/> Unknown	
<p>Approximate Downtime</p>	<input type="checkbox"/> 0 hours <input type="checkbox"/> <1 hour <input type="checkbox"/> 1-4 hours <input type="checkbox"/> 4-8 hours	<input type="checkbox"/> 8-24 hours <input type="checkbox"/> 24-72 hours <input type="checkbox"/> >72 hours	
<p>Equipment Involved</p>	<input type="checkbox"/> Industrial Controller <ul style="list-style-type: none"> <li><input type="checkbox"/> Programmable Logic Controller (PLC)</li> <li><input type="checkbox"/> Distributed Control System (DCS)</li> <li><input type="checkbox"/> Remote Terminal Unit (RTU)</li> <li><input type="checkbox"/> Intelligent Electronic Device (IED)</li> <li><input type="checkbox"/> Emergency Shutdown System (ESD)</li> <li><input type="checkbox"/> Data Acquisition Sys.</li> <li><input type="checkbox"/> Industrial Robot</li> <li><input type="checkbox"/> Smart Device</li> </ul> <input type="checkbox"/> Business Systems <ul style="list-style-type: none"> <li><input type="checkbox"/> Business Servers</li> <li><input type="checkbox"/> Desktop Computer</li> <li><input type="checkbox"/> Business Laptop</li> </ul> <input type="checkbox"/> Unknown <input type="checkbox"/> Other _____	<input type="checkbox"/> Industrial Computer <ul style="list-style-type: none"> <li><input type="checkbox"/> SCADA Master</li> <li><input type="checkbox"/> Human Machine Interface (HMI)</li> <li><input type="checkbox"/> Data Historian</li> <li><input type="checkbox"/> Programming Stn</li> <li><input type="checkbox"/> Industrial Laptop</li> <li><input type="checkbox"/> Server</li> <li><input type="checkbox"/> Simulator</li> </ul> <input type="checkbox"/> Network Hardware <ul style="list-style-type: none"> <li><input type="checkbox"/> Switch</li> <li><input type="checkbox"/> Router</li> <li><input type="checkbox"/> Printer</li> <li><input type="checkbox"/> Modem</li> <li><input type="checkbox"/> Wireless</li> <li><input type="checkbox"/> Network Media</li> <li><input type="checkbox"/> Meter</li> </ul> <input type="checkbox"/> Metering Infrastructure	

Manufacturers	<input type="checkbox"/> Controls Manufacturer <input type="checkbox"/> Allen-Bradley/Rockwell <input type="checkbox"/> Schnieder <input type="checkbox"/> Siemens <input type="checkbox"/> Emerson <input type="checkbox"/> Honeywell <input type="checkbox"/> Toshiba <input type="checkbox"/> Invensys/Foxboro <input type="checkbox"/> ABB <input type="checkbox"/> GE <input type="checkbox"/> Hunter Water Tech <input type="checkbox"/> Harris <input type="checkbox"/> Johnson <input type="checkbox"/> Telvent <input type="checkbox"/> Network Manufacturer <input type="checkbox"/> Cisco Systems <input type="checkbox"/> Enterasys <input type="checkbox"/> Nortel <input type="checkbox"/> Software-O/S Manufacturer <input type="checkbox"/> Microsoft <input type="checkbox"/> Sun <input type="checkbox"/> Wind River <input type="checkbox"/> None <input type="checkbox"/> Unknown <input type="checkbox"/> Other _____	<input type="checkbox"/>
Network Type	<input type="checkbox"/> Fieldbus/ Devicebus <input type="checkbox"/> Unknown <input type="checkbox"/> Fieldbus/ Devicebus- Asi <input type="checkbox"/> WAN <input type="checkbox"/> Fieldbus/ Devicebus- DeviceNet <input type="checkbox"/> WAN- POTS <input type="checkbox"/> Fieldbus/ Devicebus- FF <input type="checkbox"/> WAN- Private <input type="checkbox"/> Fieldbus/ Devicebus- Profibus <input type="checkbox"/> WAN- Telco ATM <input type="checkbox"/> Internet <input type="checkbox"/> WAN- Telco FrameRelay <input type="checkbox"/> Internet- VPN <input type="checkbox"/> WAN- Telco Sonet <input type="checkbox"/> LAN <input type="checkbox"/> Wireless <input type="checkbox"/> LAN- Data/Control Highway <input type="checkbox"/> Wireless- 2.4 GHz ISM <input type="checkbox"/> LAN- Ethernet <input type="checkbox"/> Wireless- 802.11 WiFi <input type="checkbox"/> None <input type="checkbox"/> Wireless- 900 MHz ISM <input type="checkbox"/> Serial <input type="checkbox"/> Wireless- BlueTooth <input type="checkbox"/> Serial- Local Connection <input type="checkbox"/> Wireless- InfraRed <input type="checkbox"/> Serial- Modem Dialup <input type="checkbox"/> Wireless- Licensed Connection <input type="checkbox"/> Wireless- Microwave <input type="checkbox"/> Serial- Modem Leased Line <input type="checkbox"/> Other _____ Connection	
Protocols Involved	<input type="checkbox"/> AB Data Highway + <input type="checkbox"/> Other <input type="checkbox"/> AB PCCC/DF1 (DH+) <input type="checkbox"/> Profibus FMS <input type="checkbox"/> DNP3 <input type="checkbox"/> SMTP <input type="checkbox"/> Ethernet/IP <input type="checkbox"/> SNMP <input type="checkbox"/> Fieldbus FMS <input type="checkbox"/> SQL <input type="checkbox"/> FTP <input type="checkbox"/> TCP/IP <input type="checkbox"/> HTTP <input type="checkbox"/> Telnet <input type="checkbox"/> Industrial Application <input type="checkbox"/> Unknown <input type="checkbox"/> MODBUS	

<b>Incident Description</b>	
Please describe in detail what happened. Make sure you include any items of interest not covered on the previous pages as you fill out this section.	
Describe the incident in general terms.	
What was the impact on your organization?	
What did you do to make sure it would not happen again?	
Any public references on this incident? (Web URL's, public records, etc).	
Comments :	<input type="checkbox"/>

**Fax or email all sheets to 215-257-1657 or [submit@securityincidents.org](mailto:submit@securityincidents.org)**

**Attention: RISI Database Administrator**