



# Roadmap to Secure Control Systems in the Water Sector

## Vision

In 10 years, control system for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.

Challenges			
<ul style="list-style-type: none"> <li>■ Limited collaboration between IT and ICS departments</li> <li>■ Limited executive recognition of ICS security threats &amp; liabilities</li> <li>■ Business case for ICS security is not established</li> </ul>	<ul style="list-style-type: none"> <li>■ No clear up-front security requirements</li> <li>■ Limited understanding of ICS risk factors</li> <li>■ Rapid pace of change in threat actions &amp; vulnerabilities</li> <li>■ No ICS security training resources</li> </ul>	<ul style="list-style-type: none"> <li>■ Limited resources to mitigate risk</li> <li>■ Difficult or impossible to integrate new technologies into legacy systems</li> <li>■ Managing change in mission critical systems</li> </ul>	<ul style="list-style-type: none"> <li>■ Differing viewpoints of sector partnerships</li> <li>■ Competing priorities limit resources</li> <li>■ Difficult to fully implement cyber-security across entire water sector</li> </ul>

Goals			
Develop and Deploy ICS Security Programs	Assess Risk	Develop and Implement Risk Mitigation Measures	Partnership and Outreach

Milestones			
Near Term (0-1 Years)			
<ul style="list-style-type: none"> <li>■ 80% of water sector executives recognize ICS security is mission critical</li> <li>■ IT staff and ICS engineers and operators coordinate ICS security efforts</li> <li>■ Integrate security as a key goal in every project plan</li> <li>■ Develop a recommended practices ICS security template for widespread use in the water sector</li> <li>■ Integrate &amp; elevate ICS security requirements with vendor contracts</li> <li>■ Isolate ICS from public switched networks</li> <li>■ Integrate roadmap with Water Sector Specific Plan</li> </ul>	<ul style="list-style-type: none"> <li>■ Develop ICS risk assessment &amp; reporting guidelines published and available throughout the water sector</li> <li>■ Identify common metrics for benchmarking ICS risk (threat-vulnerabilities-consequence) in the water sector</li> <li>■ Develop ICS risk assessment tools, such as end-to-end, threat-vulnerabilities-consequence analysis capability for the water sector</li> </ul>	<ul style="list-style-type: none"> <li>■ Establish working group for developing and maintaining recommended practices for ICS security for ICS network architecture(s) for the water sector</li> <li>■ Develop cyber response protocol template</li> <li>■ ICS vendors start to implement or increase their cyber security features by 50%</li> <li>■ Identify and implement existing security features built into the devices</li> <li>■ Replace default security passcodes</li> </ul>	<ul style="list-style-type: none"> <li>■ Develop effective federal &amp; state incentives to accelerate investment to secure ICS technologies and practices</li> <li>■ Increase ICS security awareness between water sector, cross-sector, vendor and commercial partners</li> <li>■ Develop essential body of ICS security knowledge for information sharing</li> </ul>



<b>Mid Term (1-3 Years)</b>			
<ul style="list-style-type: none"> <li>■ Conduct sector-wide training on recommended practices ICS security template</li> <li>■ Integrate ICS security awareness, education &amp; outreach programs into water sector operations</li> </ul>	<ul style="list-style-type: none"> <li>■ Conduct sector-wide training on risk assessment tools</li> </ul>	<ul style="list-style-type: none"> <li>■ Reduce installation time of ICS patching                             <ul style="list-style-type: none"> <li>- Firmware by 50%</li> <li>- Applications by 99.9%</li> </ul> </li> <li>■ System design accommodates restarts</li> <li>■ Develop operator ICS security training program</li> </ul>	<ul style="list-style-type: none"> <li>■ Adopt recommended practices for ICS security in the water sector</li> <li>■ Develop public communication channels to increase confidence in efforts to prevent or minimize impacts from a cyber event</li> </ul>
<b>Long Term (3-10 Years)</b>			
<ul style="list-style-type: none"> <li>■ Sustain roadmap activities in accordance with the Water Sector Specific Plan</li> </ul>	<ul style="list-style-type: none"> <li>■ Water sector actively measures ICS security performance and benchmarks with other sectors</li> </ul>	<ul style="list-style-type: none"> <li>■ Develop and implement self-defending ICS &amp; infrastructure</li> <li>■ Require ICS security in operator certification</li> <li>■ Real-time security state monitoring for intrusions are commercially available</li> </ul>	<ul style="list-style-type: none"> <li>■ Establish life cycle investment &amp; framework for cyber security</li> <li>■ Government maintains ICS threat support</li> <li>■ Identify, understand &amp; disseminate timely ICS risk information within the sector &amp; among its partners</li> </ul>
<b>End State (2015)</b>			
The water sector will have ICS security programs that reflect changes in technologies, operations, standards, regulations, and threat environments	The water sector will have a robust portfolio of ICS recommended security practice analysis tools to effectively assess risk	Security solutions for legacy system, new architecture designs, and secured communication methods will be cost effective	Water asset owners and operators will work collaboratively with government and sector stakeholders to accelerate security advances



16 Chestnut Street · Suite 300  
 Foxborough, MA · USA · 02035  
 T: +1-508-718-6700  
 F: +1-508-718-6701  
 E: [info@industrialdefender.com](mailto:info@industrialdefender.com)  
[www.industrialdefender.com](http://www.industrialdefender.com)