PRESS RELEASE

CYBER REGULATION FACT SHEET SHOWS GOVERNMENT MANDATES ARE COUNTER-PRODUCTIVE

(WASHINGTON, D.C.) – The Internet Security Alliance today released a "Cyber Regulation Fact Sheet," demonstrating multiple examples of how the tremendous growth in cybersecurity rules and regulations is diverting scarce security resources and actually undermining our nation's cyber defenses.

"One of the unintended consequences for organizations, like ISA who has been raising awareness of the cyber threat for 15 years, is that we now have cyber mandates springing up like weeds as virtually every governmental entity, federal state and local, fight to be the 'cyber guy'. The result is an uncoordinated, inconsistent and often counterproductive set of requirements that actually hurts, not helping, increased security," said ISA President Larry Clinton.

"Research tells us we are experiencing more than a million cyber-attacks a year and we don't have nearly enough cyber professionals to help protect us. We need to use our scarce resources efficiently and effectively," Clinton said. "Yet some firms are now spending 30 percent of their budgets and 40 percent of their time of various compliance regimes, none of which have been shown to empirically aid in securing our cyber systems."

ISA's fact sheet offered numerous examples from multiple industry sectors of the growth of cyber regulations often inconsistent with the risk management philosophy that professionals overwhelmingly suggest is a more effective approach to cyber defense. Among the statistics cited are:

- In the financial services sector, increases of over 300% in cybersecurity and privacy related questions financial institutions now need to answer.
- In the defense sector, there are new rules for unclassified controlled information that force companies to label bits of information based on 23 categories, 84 sub-categories, and hundreds of different citations. Ironically, these rules could actually make it easier for attackers to find useful data.
- In Energy, DOE has proposed requirements (10 CFR 73.53) that all networks in the sector meet controls (DG 5062) so overly broad that the mandate will require the expenditure of millions of dollars to implement controls not tailored for the risk of the networks.
- New defense acquisition rules will require small companies to comply with extraordinary detailed requirements that may well drive many smaller firms out of the defense business, which is both inconsistent with DoD policy to promote the use of smaller companies as well as harms national security, as many of these firms are the top suppliers who can find markets for their services that don't require the extensive compliance.
- Various regulators are demanding public disclosure of supposedly material cyber-attacks when in fact the attack itself may not have a material effect. But, the disclosure may well trigger unjustified (and usually temporary) stock fulgurations. Thus, it is the disclosure creating the material effect and provides a path for stock manipulation contrary to the regulator's mission.

"No one, certainly not ISA, is saying we ought not to have cyber controls or assessments. But, we need to have a rational and well-thought out system or we will waste vital resources and undermine our security," said Clinton

###