INTERNET SECURITY ALLIANCE

Overview of ISA programs and services

March 22, 2011

ISA Board of Directors

Ty Sagalow, Esq. Chair, Executive Vice President & Chief Innovation Officer, Zurich North America
Tim McKnight, 1st Vice Chair, Vice President & Chief Information Security Officer**,** Northrop Grumman
Jeff Brown, **Secretary / Treasurer**, Vice President, Infrastructure and Chief Information Security Officer, Raytheon

- Pradeep Khosla, Founding Director of Cylab, **Carnegie Mellon University**
- Marc Sachs, Vice President Government Affairs**, Verizon**
- Lt. Gen. Charlie Croom (Ret.), Vice President Cyber Security, Solutions **Lockheed Martin**
- Eric Guerrino, Managing Director Systems and Technology**, Bank of New York Mellon**
- Joe Buonomo, President**, DCR**
- Bruno Mahlmann, Vice President Cyber Security Division**, Dell**
- Kevin Meehan, Vice President Information Technology & Chief Information Security Officer**, Boeing**
- Rick Howard, iDefense Manager**, VeriSign**
- Justin Somaini, Chief Information Security Officer, **Symantec**
- Gary McAlum, Chief Security Officer**, USAA**
- Paul Davis, Chief Technology Officer, **NJVC**
- Andy Purdy, Chief Cybersecurity Strategist**, CSC**
- John Havermann, II, Vice President & Director, Cyber Programs , Intelligence & Information**, SAIC**

ISAlliance Mission Statement

ISA seeks to integrate advanced technology with economics and public policy to create a sustainable system of cyber security.

ISA history and thought leadership timeline

2000

- ISA founded by former Chair of the U.S. House Intelligence Committee and CMU

2001

- ISA provides exclusive private sector access to the knowledge base on internet threats and vulnerabilities at CERT/CC

2002

- ISA published best practices for information security targeted to senior corporate managers.

2003

- ISA published its first set of best practices for mobile executives.

2004

- ISA Publishes its first best practices to prevent insider threats.
- The National Cyber Summit asked ISA to fill in one of the major cyber security gaps and develop a set of best practices for cyber security for small businesses.

2005

- ISA chairs the Cong. Apt. Cross Sector Cyber Security Working Group on market incentives

2006

- ISA in collaboration with Carnegie Mellon University launched its first effort to secure the IT supply chain.

2007

- ISA launched its first effort with ANSI to provide guide on financial risk of cyber events.

ISA history and thought leadership timeline

2008

- ISA published its first Social Contract for Cyber Security, which provided model for private-public partnership.
- ISA publishes compliance guide for digital tech & analog laws & regs
- ISA Publishes Framework for Supply Chain Management

2009

- President Obama publishes “Cyber Space Policy Review” Ex. Summary begins and ends with ISA Social Contract ---14 other ISA White Papers cited---more than any other source.
- ISA selected by the U.S. State Dept. to brief the NATO Cyber Excellence Center and EU Commission on Cyber on the Social Contract approach
- ISA Publishes 50 Questions Every CFO Should ask @ Cyber Security

2010

- ISA published the “The Financial Management of Cyber Risk” in collaboration with ANSI.
- At the White House, with President Obama in attendance, U.S. Commerce Department Secretary Locke cited the ISA security checklist for smart phones as one of the major accomplishments in cyber security that year

2011

- ISA joins with coalition BSA, US Chamber, Center for Democracy and Technology and Tech America White Paper on Cyber Security Policy

2008-11 Three Year Plan Goals

- Provide meaningful thought leadership on information security
- Represent industry before legislators and government agencies, notably DHS
- Create mechanisms for rapid development and implementation info security practices policies and technologies
- Grow & Strengthen ISA

2012-15 Plan (written in 2011) Possible Projects

- Integrate disparate cyber supply chain programs
- Hold event with all sectors showing BP for supply chain
- Monthly targeted Hill briefings
- Update ISA past best practices
- Consolidate ISA members educational programs

Possible new projects

- Create web-based service for world wide info on cyber laws/standards
- ISA web access to member companies best practices and services free for small businesses
- Video for Financial Risk Management
- Initiate Training programs based on ISA products
- Creative Education in cyber security

2008-2011 Objectives

- Improve industry advocacy via working with other organizations
- Move ISA mission statement into the public discussion & govt. policy
- Provide model for PPP using incentives
- Improve advocacy with current projects and create new ones
- Expand opportunities for members to show thought leadership

2008-2011 Objectives

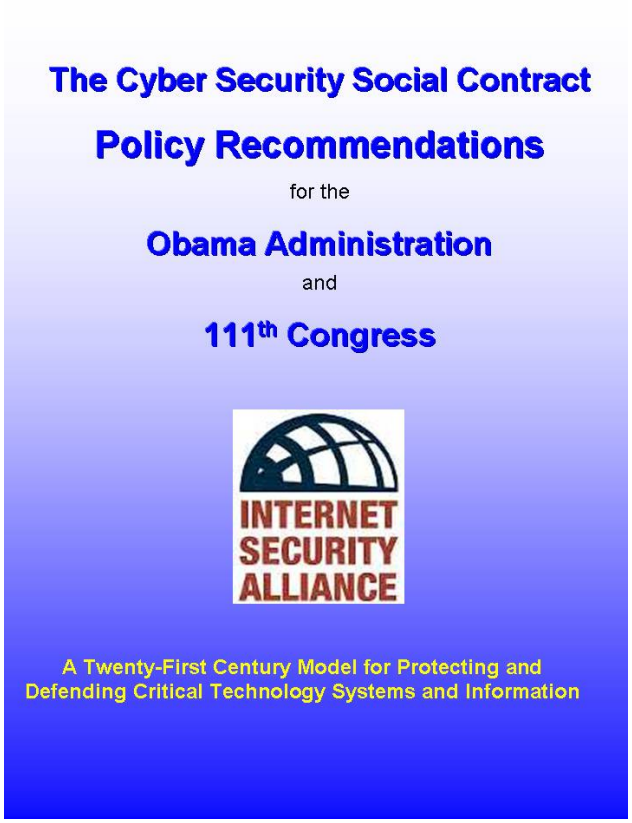
- Initiate and maintain program on enterprise cyber risk management
- Initiate a program on standards for (VOIP)
- Expand supply chain program
- Establish international program
- Reach to underserved communities

ISA Priority Programs

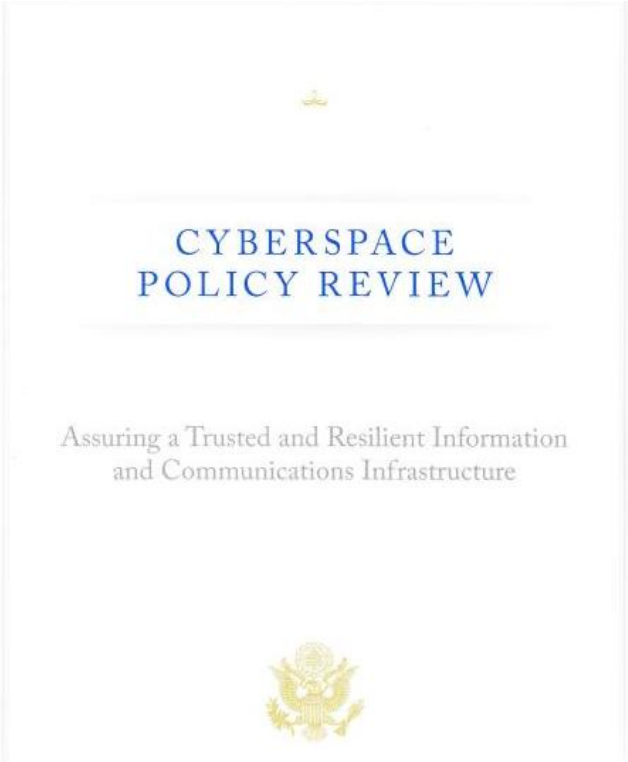
- Security standards for VOIP-Smart Phones CCP
- Securing the Global IT Supply Chain
- New model for information sharing
- Navigating compliance with advanced technology and multiple jurisdictions
- The Cyber Security Social Contract (partnership model for industry and govt. based on market principles)
- Corporate financial risk management of cyber security

ISA Cyber Social Contract

- Similar to the agreement that led to public utility infrastructure dissemination in 20th Century (RoR regulation)
- Infrastructure development -- market incentives.
- We know what to do technically & operationally, but the economics & strategy are not in place
- Partner at the business plan level and apply market Incentives from rest of the economy to cyber



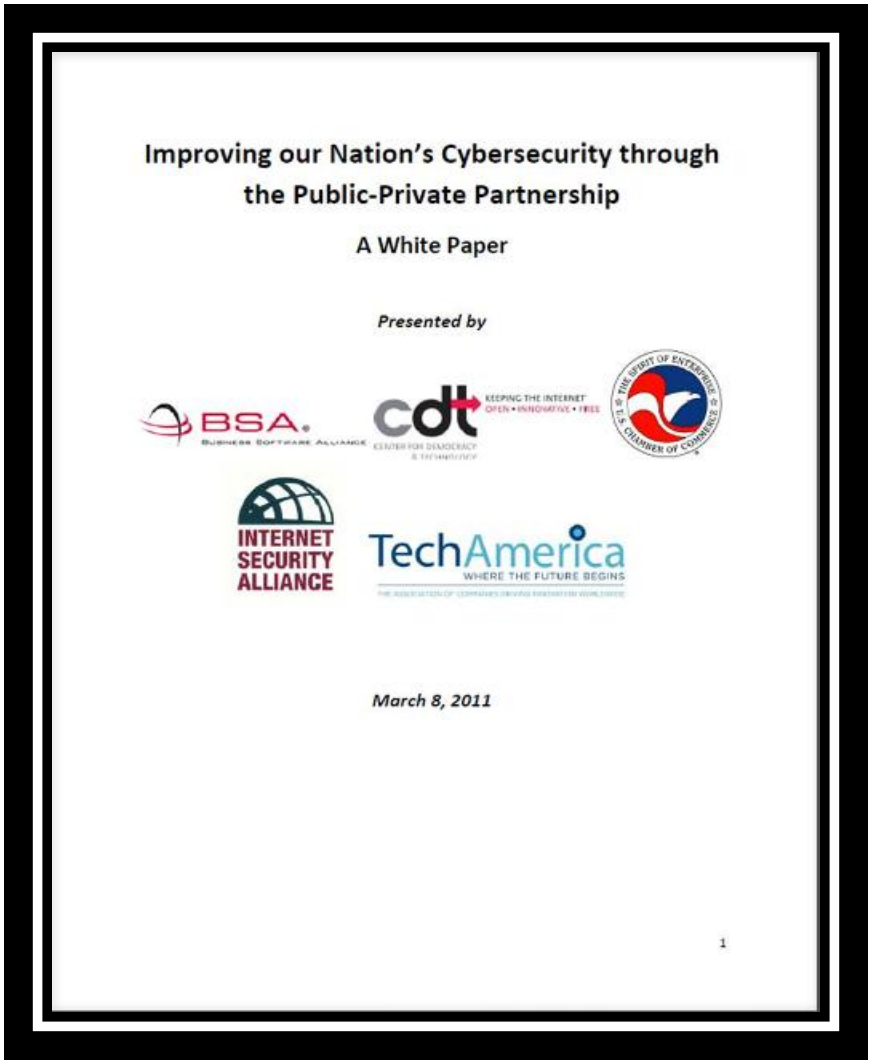
President Obama's Report on Cyber Security



- The United States faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights. (President's Cyber Space Policy Review page iii)

- Quoting from Internet Security Alliance Cyber Security Social Contract: Recommendations to the Obama Administration and the 111th Congress November 2008

Public policy advocacy


Improving our Nation's Cybersecurity through the Public-Private Partnership

A White Paper

Presented by

BSA. Business Software Alliance

cdt Keeping the Internet Open • Innovative • Free. Center for Democracy & Technology

U.S. Chamber of Commerce

INTERNET SECURITY ALLIANCE

TechAmerica Where the future begins

March 8, 2011

1

Joint trade association white paper on public-private partnerships

- Cooperative effort between ISA, US Chamber, Business Software Alliance, Tech America and Center for Democracy and Technology
- House and Senate briefings held March 11
- Met with Howard Schmidt on March 21

Public Policy - White House

- Started with Schmidt meeting in August 2010
  - Trade Association Paper was in process
  - Goals
    - Support enhanced P-P Partnership model
    - Help private sector set agenda for cyber legislation
    - Provide support for our allies

Legislative activity

- Momentum building on cyber issues
  - Sen. Reid met with committees of jurisdiction chairs March 15—comp. approach
  - House wants smaller bills
  - Sen. HLS & Rep. Langevin introduced legislation
  - WH will issue report in April

Public Policy Next Steps

- ISA continues to meet with members and staff, building on extensive groundwork this past fall and winter
- Craft specific language capturing our public policy priorities
- Continue to build relationships and emphasize the importance of cyber security issues
- Create programming for cyber security caucus members
- Hold briefings for White House and Congressional staff members

INTERNET SECURITY ALLIANCE

Supply chain project

- Initiated in 2006 in partnership with CMU
- Project leader is Scott Borg, US Cyber Consequences Unit
- Workshops have led to a comprehensive list of standards and practices to be published at the end of Q2
- Workshops on design, fabrication, pre-assembly, distribution and maintenance

Supply chain project

- Next workshop will cover legal and contractual conditions for implementing security measures
- ISA is looking for participants
- Project will be entering new phase

INTERNET SECURITY ALLIANCE

VoIP Project

- **Development of the Baseline Security Configuration Checklist for IP Phones**
  - Vendor independent security configuration guidelines
- **Security Configuration Checklist for Microsoft Office Communications Client**
  - Preliminary configuration policies documented
- **Public Awareness of SCAP Applicability for VoIP**
  - Presentation at 6th Annual IT Security Automation Conference
- **Interest Expressed by Product Vendors**

VoIP Goals and Objectives for 2011

- **Continue focus on industry adoption of SCAP for VoIP**
  - Submission of Microsoft Office communication client checklist to National Checklist Program in 1Q'11 (this will be the industry's first VoIP application in NCP)
  - IETF participation
- **Stronger collaboration with product vendors**
- **Target the end-user; drive SCAP content development through user demand**
  - Author paper to highlight benefit of SCAP-enabled VoIP devices

INTERNET SECURITY ALLIANCE

Information Sharing

- Current model needs to be updated
- Modern business systems too open
- Limited participation in ISACs especially SMEs
- Gov won't give source material, industry won't give attack data or important internal information
- Can't keep out determined attackers
- Once in the systems we have more control over attackers

Information Sharing – Incentives

- Large Orgs become designated reporters (gold, silver etc.) which can be used for marketing
- Rpt C2 sites, (URLs-web sites) not that they have been breached or internal data
- Gov reports – not source data
- AV community circulate the info for profit
- Small companies able to participate easy and cheap to block C-2
- Working w/DHS and InfraGard to implement

Financial Management of Cyber Risk

- ISA has worked with ANSI to assist organizations in developing an enterprise-wide risk management approach to cyber security
  - "The 50 Questions Every EFO Ought to Ask About Cyber Security"
  - "The Financial Management of Cyber Risk: An Implementation Framework"

Financial Management of Cyber Risk

- Project is entering phase III
  - ISA outreach to business organizations, working with Melissa Hathaway
  - Next step is to elevate the issue to the CEO/ CFO/board member level
  - Advanced Persistent Threat
    - Targets individuals within an organization
    - Awareness is high with recent media coverage
    - Presents an opportunity for C-level education program

Ways to become involved

- Participate in one (or more) of our projects
  - Projects are often carried out through a series of workshops
- Members are our subject matter experts
  - Public policy
  - Emerging issues
  - More effective ways to partner with government
- Contact us!

Larry Clinton
President & CEO
Internet Security Alliance
lclinton@isalliance.org
703-907-7028
202-236-0001

www.isalliance.org