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

Board of Directors

Ty Sagalow, Esq. Chair President, Innovation Division, Zurich
J. Michael Hickey, 1st Vice Chair VP Government Affairs, Verizon
Tim McKnight Second V Chair CSO**,** Northrop Grumman

- **Joe Buonomo**, President, DCR
- **Jeff Brown**, CISO/Director IT Infrastructure, Raytheon
- **Lt. Gen. Charlie Croom (Ret.)** VP Cyber Security, Lockheed Martin
- **Paul Davis**, CTO, NJVC
- **Eric Guerrino,** SVP/CIO, Bank of New York/Mellon Financial
- **Pradeep Khosla**, Dean Carnegie Mellon School of Computer Sciences
- **Bruno Mahlmann**, VP Cyber Security, Dell
- **Gary McAlum,** CSO, USAA
- **Kevin Meehan**, VP & CISO, Boeing
- **Andy Purdy**, Chief Cybersecurity Strategist, CSC
- **Ken Silva**, CSO, VeriSign
- **Justin Somaini**, CISO Symantec

Legislative Intent: Senate Consolidated Draft

- "**Summary: HSGAC-Commerce Staff Draft Cybersecurity Bill**
- The bill creates a dynamic partnership between the government and private sector in which the private sector is responsible for enhancing security of the Nation's most critical systems while the government ensures effective oversight and compliance."

Obama: What We Need to Do

It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts.

Obama Administration Cyber Space Policy Review
May 30, 2009 page 15

ISA The Framework of Supply Chain Attacks

4 kinds of cyber attacks that are possible at each stage of the supply chain:

- Cyber attackers could interrupt the operation.
- Cyber attackers could corrupt the operation (including inserting malware).
- Cyber attackers could discredit the operation (undermining trust, damaging brand value).
- Cyber attackers could undermine the basis for the operation (loss of control, loss of competitively important information).

ISA The Framework of Supply Chain Attacks

Remedies to Supply Chain attacks

1. Protection against interruption:
   - Continual, mandatory sharing of production across supply chain.
   - Maintaining alternative sources.
2. Protection against insertion of malware:
3. Strict control of environments where key intellectual property is being applied.

ISA The Framework of Supply Chain Attacks

Remedies to Supply Chain attacks

4. Logical tamper-proof seals.
5. Physical tamper-proof seals.
6. Effective sealing and tracking of containers.
7. Protection against undermining trust:

ISA The Framework of Supply Chain Attacks

Remedies to Supply Chain attacks

8. Logging of every operation and who is responsible.
9. Protection against loss of control of information:
10. Versioning as a tool for protecting intellectual properties.

ISA The Framework of Supply Chain Attacks

Five different supply chain stages to which the remedies need to be applied:

I. The Design Phase.

II. The Fabrication Phase.

III. The Assembly Phase.

IV. The Distribution Phase.

V. The Maintenance Phase.

ISA The Framework of Supply Chain Attacks

If we combine the list of remedies with the stages of the supply chain to which they need to be applied, we get a "Remedies for Stages Grid."

REMEDIES

STAGES				

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

www.isalliance.org