

INTER • PACT

11511 Pine Street
Seminole, Florida 34642
Fon: 813-393-6600 • Fax: 813-393-6361 • E-mail: PO0506 @ pallink.com

William Schwartz
Executive Director

August 2, 1994

Robert Steele
OSS, Inc.
11005 Langton Arms Ct.
Oakton, VA 22124

at 703-242-1711

Robert,

In response to the request of how to allocate budgetary funds for security concerns as they relate to the NII, I offer the following thoughts for your consideration.

1. 10% to establish and operate a cooperative (government and commercial) independent private organization to establish the scope of security and privacy standards as they apply to potential threats to the NII today and in the future.
2. 15% to establish independent testing and certification laboratories to verify the efficacy of information security products.
3. 15% for an aggressive high profile, education and awareness training program aimed at both the government and private sector as to the risks and vulnerabilities of the NII and methods of protection.
4. 25% to establish electronic privacy guidelines and models, and implement them across critical government systems such as the IRS, SSA, VA. To be used as model for private sector. Privacy begets security.
5. 35% to secure and oversee the administration of government systems which have electronic connections to the unclassified world.

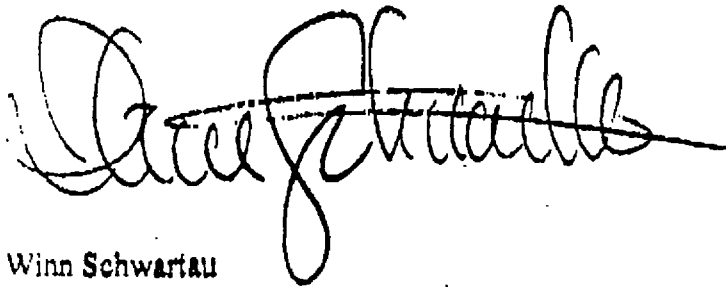
I see these items as working in synergistic concert to lay the foundation for NII security. Much of this is ground breaking and far reaching work but is eminently do-able in a reasonably short time.

Central to the themes I propose is a cooperative academic/practical approach to the wide spread implementation of information security and privacy solutions. Historically the government and academic approach is viewed as "impractical" and not real-world enough. The private sector has too much self interest to police itself. A Federal Reserve Board style organization would ideally strive to meet the real-worlds needs of the commercial sector and the majority (not secret military) of the government.

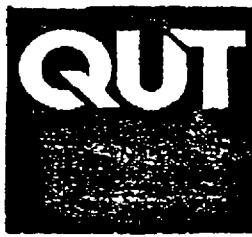
The current battles only exacerbate the tension and achieve little.

I hope these comments have some value in your endeavors. I'll be happy to make whatever changes you feel are appropriate.

As usual, all the best to you and your family.

A handwritten signature in black ink, appearing to read "Winn Schwartz". The signature is written in a cursive style with a horizontal line crossing through the middle of the letters.

Winn Schwartz
Executive Director,
Inter.Pact



Mr R Steele
 President
 Open Source Solutions, Inc.
 11005 Langton Arms Court,
 Oakton, Virginia. 22124-1807
 U.S.A.

Fax : +1 - 703 - 242 1711

22 July 1994

Dear Robert,

Good to talk with you yesterday and to receive the copy of your "Testimony and Comments" to the NII Task Force.

I attach some "bullet points" for consideration as well as a separate set of thoughts that support those "bullet points".

My key theme is that business interests are now global, particularly in the information and services sectors of national economies and of the United States in particular. The change in the US economy to a services and information sector based economy most likely occurred there in the late 1960s but it could have been earlier. We knew that by the 1970s most US jobs were in the services and information sectors, i.e. over 50% of designated job activities.

The problem was that Commerce did not really study the change that closely till much later. Thus information infrastructure underlying the new commercial base of the USA's GDP is the new and major military and strategic factor in any defence "equation". This also may not have been recognised by the military itself, e.g. the 1980s "Star Wars"/SDI of the Reagan administration, etc and definitely NOT by commercial government departments and agencies in the USA!

**Information Security Research Centre
 Queensland University of Technology**

ens
 107 864 2800
 171 221 2384

QUT Kelvin Grove
 Victoria Park Road
 Locked Bag No 2
 Red Hill Q 4068
 Australia
 Phone: (07) 864 2111
 Fax: (07) 864 3988

QUT Kedron Park
 Kedron Park Road
 PO Box 117
 Kedron Q 4001
 Australia
 Phone: (07) 864 2111
 Fax: (07) 864 4488

QUT Carlseldine
 Beams Road
 PO Box 284
 Zillmere Q 4034
 Australia
 Phone: (07) 864 2111
 Fax: (07) 864 4998

QUT International
 Codes
 Central Administration
 Phone +61 7 864 2111
 Fax +61 7 864 1810

PLEASE REPLY TO THE GARDENS POINT ADDRESS

(Incidentally, this latter point was clearly acknowledged at last year's NCSC conference in Baltimore when the FISSEA - Federal Security Education - group clearly identified that of the designated, full-time INFOSEC positions within the United States Government and its agencies, almost ALL were in the military sector with less than one designated and funded INFOSEC position per commercial Government Department / Agency identified).

Incidentally, could you ask your secretary to note that my fax number here, and the number to be used, is :

Country Code : 61
City Code : 7
Number : 221 2384

The number previously used is the general fax number for the University and is another building in a very public area. The above number is in a secure area in the Information Security Research Centre.

Best wishes,



Professor William J Caelli, FACS, FTICA
Professor and Head,
School of Data Communications

and

Acting Chairman
Technical Committee 11
International Federation for Information Processing

Suggested program Name : Info Guardian

- Information Infrastructure strategic assessment and valuation programme
 - assessment of contribution to GDP of NII dependent sections of the economy
 - vulnerability analysis of NII "backbone" structures and services

(Solution : Expansion of DoD strategic assessment role, through extension of the charter of existing analysis groups and/or divisions, to incorporate political, economic and social aspects of commercial level NII based activity as well as military significance of such infrastructures.)

- Determination of the technologies and management organisations needed for protection "gateways" and associated structures required to defend the national Information Infrastructure (NII) from the required International/global Information Infrastructure (GII) Interconnection.

- Technology assessment and prototype development for "guarded" access to/from the GII, including "learning" nodes capable of identifying and rejecting attacks.

- Protection technologies for the high-speed, broadband services providing the back-bone to the NII

- Specific defence technologies required to protect the NII from attack from both external and internal sources, including:
- Technology requirements for confidentiality, integrity and continued and guaranteed availability of NII services.

(This includes determination and prototype development of deployable ultra high speed cryptographic and steganographic technologies capable of coping with ATM - Asynchronous Transfer Mode - telecommunications disciplines, the suggested basis for the NII and for all planned carrier services, as a minimum.)

- * Expansion of analysis role of the appropriate DoD agencies to incorporate assessment, analysis, re-definition and development of existing and planned financial and allied message formats and transmission protocols, including any security related technologies and protocols, to enable the secure integration of national financial information services into the Nil/Gil schemes.

- * Identification and development of the necessary management processes and technologies to protect identified key Nil Infrastructure components, including :
 - national "backbone" telecommunications switching hubs,
 - interconnections to/from such hubs.

- * Identification and development of next generation protection technologies for commercial level telecommunications infrastructure components including:
 - software sub-systems associated with major components of the Nil,
 - hardware protection technologies for telecommunications bearers, including radio/microwave transmission based services, fibre-optic bearers/cables, etc.
 - identification of components that may be supplied by Defence contractors, based upon DoD designs, which meet commercial requirements and acceptability.

THIRD INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL
COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1994 Volume I -
[Link Page](#)

[Previous](#)

[Correspondence to the National Information Infrastructure Security Committee: CROSS-WALK OF THREE SECURITY EXPERTS' RECOMMENDATIONS FOR SPENDING SIB/YEAR FOR NII SECURITY PROGRAM](#)

[Return to Electronic Index Page](#)