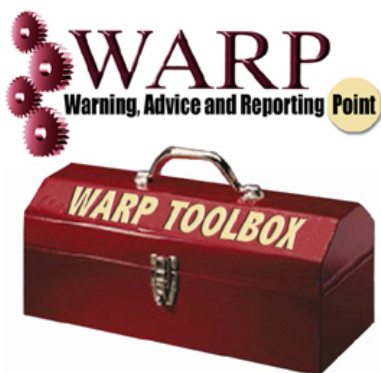


Network Security – challenges for world class events

WARPs

and the 2012 Olympics

(Warning, Advice and Reporting Points)



John Harrison,
Consultant to
NISCC.

What, Why, When and How



- **What** - is a WARP
- **Why** - do London 2012 Olympics need a WARP
- **When** - do they need a WARP
- **How** - can this WARP be provided

WARP Vision

WARPs - becoming endemic

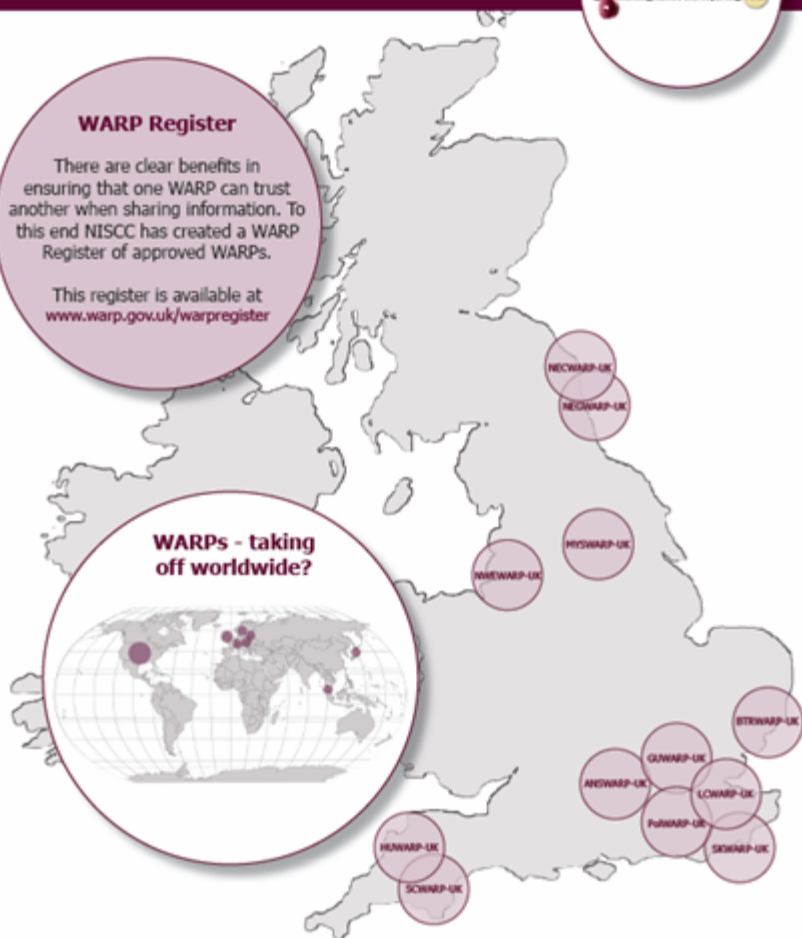
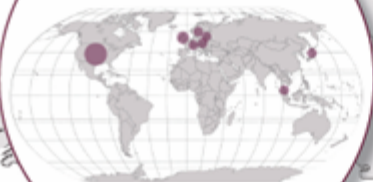


WARP Register

There are clear benefits in ensuring that one WARP can trust another when sharing information. To this end NISCC has created a WARP Register of approved WARPs.

This register is available at www.warp.gov.uk/warpregister


WARPs - taking off worldwide?




WARP Benefits for the Olympics


- Creating Awareness
- Better Protection of large investment in ICT systems
- Filtering service for Warnings & Advisories
 - Customised to meet needs of Olympiad community
 - Cost effective
 - Targetted delivery
- Network for advice, contacts and sharing Best Practice
- Highly Relevant Early Warnings
- Learn from other WARP communities
- Reduced threat to everyone else

Filtered Warnings Application



WARP
Warning, Advice and Reporting Point





Home
My Details
My Subscription
News
Alerts

My Services

- My Subscription
- Alert Chronicle
- News Chronicle
- My Details

News

- News Management
- New News

Latest Five Alerts

Low Severity Warning

Virus warning - W32/Bagz-D

Low Severity Advisory

Bypassing MS Windows XP SP2 firewall

Normal Severity Advisory

Multiple Vulnerabilities in Microsoft Internet Explorer

Low Severity Advisory


Sun Solaris LDAP and RBAC Privilege Escalation Vulnerability


Low Severity Advisory

RIM Blackberry Meeting Request Message "Location" Header DoS

Subscription Tree

Please select the categories of interest to you. To select a category or branch, simply tick the branch and all the items under it will be selected.

 This means there are one or more items under a certain branch.

 This item has been selected but you have not selected any other items.

- All Categories
- Good Practice
- Incident/Threat
 - Target Groups
 - Incident Types
 - Motive & effect
 - Threat types
- Vulnerabilities/Fixes
 - Cisco
 - HP
 - Linux/Apache
- Microsoft
 - MS Bundled Windows Software
 - MS Developer Products
 - MS Office/Business Products
 - MS Home Products
 - MS Server Products
 - MS Windows Operating Systems
 - Windows CE
 - Windows 2000
 - Windows XP
 - Windows 3.x
 - Windows 95
 - Windows 98
 - Windows NT
 - Windows 2003
- Sun Microsystems
 - Apple

You are: [Home](#) | Home

[News](#) | [Our city](#) | [Our country](#) | [Our vision](#) | [Getting involved](#) | [Search](#) [Go](#)

London 2012 images

View images of the London 2012 Games, including artists' impressions of the Olympic Park.

[View picture gallery](#)

Quick links

[Information for your business](#)

[Use of Olympic Marks](#)

[Avoid e-mail scams](#)

[Our Singapore Presentation](#)

[Interactive venue guide](#)

[Register your interest as a volunteer](#)

[Sign up to receive our e-newsletter](#)

[Olympic Stadium images](#)

[Read the Candidate File](#)



Countdown to London 2012



[The 1908 London Olympics](#)
Tell me more >

[Business and London 2012](#)
Click here to find out more >



Partnerships key to Games success

26 May: ODA Chief Executive David Higgins has spoken about the importance of partnerships in ensuring the success of the London 2012 Games.

[Partnerships - read more](#)



Daley to train young athletes

23 May: Daley has been called to train young British athletes ahead of the London 2012 Games.

[Daley Thomas - read more](#)

Vacancies

[Click here to view roles at ODA](#)

[To register to receive London 2012's e-newsletter](#)



Avoid e-mail scams

You are: [Home](#) | [Our vision](#) | [Security](#)

[News](#) | [Our city](#) | [Our country](#) | [Our vision](#) | [Getting involved](#) | [Search](#) [Go](#)

- [LOCOG](#)
- [ODA](#)
- [Our Bid](#)
- [Interactive map](#)
- [The Olympic Park](#)
- [Sports and venues](#)
- [The Paralympics](#)
- [Best-ever Games transport](#)
- [A sustainable Games](#)
- [A lasting legacy](#)
- [Olympism and culture](#)
- [Total Government support](#)
- [Accommodation](#)
- Security**
- [The UK's Games](#)



Unrivalled security expertise

The sight of the Bobby on the beat is as familiar to tourists as Trafalgar Square and Big Ben.

But the Met also boasts unsurpassed expertise in managing major events safely and unobtrusively.

In 2003 they policed 4,500 public and 460 sporting events in addition to 40 ceremonial occasions, including the Rugby World Cup victory parade.

And every year nearly 1m people attend the world-famous Notting Hill Carnival - the world's largest street party and a spectacular celebration of London's diversity as well as a byword for successful community policing.

The UK security services also already have experience of the specific challenges of hosting an Olympic Games. As chair of the Olympic Security Advisory Group, the UK was instrumental in ensuring that the Athens Games passed off safely and successfully.

For 2012, the Met is working closely with London 2012 on an all-encompassing security plan in which counter-terrorism, crowd management, general policing and other measures will be developed in line with established public safety strategies.

Its full resources, now in excess of 30,000 officers, as well as regional police forces and other policing agencies, would be dedicated to ensuring a safe and secure environment in 2012 for athletes and spectators alike.

Already, Met experts are giving specialist advice to architects and masterplanners to ensure not only a safe and secure Games, but a safe and secure, crime-free, environment for the future.

[London 2012 Candidate File Theme 12: Security](#)

Sporting venues
What's planned and where
[Find out more >](#)



The 1908 London Olympics
[Tell me more >](#)

The ODA
[Click here to learn more >](#)



Backing the Bid:
Joanna Lumley

"Anything that helps young people become more involved in the arts, culture, sport and the spirit of personal achievement excites me. The Olympics isn't only a sporting feast - it's a celebration of culture and creativity too - and that gets my vote."

US Cybernotes 2003 – page 1



Department of Homeland Security Information Analysis and Infrastructure Protection Directorate CyberNotes

Issue #2003-26

December 31, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a year-end summary of software vulnerabilities identified between December 6, 2002 and December 12, 2003. The table provides the vendor, operating system, software name, common name of the vulnerability, potential risk at the time of publication, and the CyberNotes issue in which the vulnerability appeared. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source indicated in the endnote.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold.** New information contained in the update will appear in italicized colored text. Where applicable, the table lists a "CVE number" (in red)

NISCC

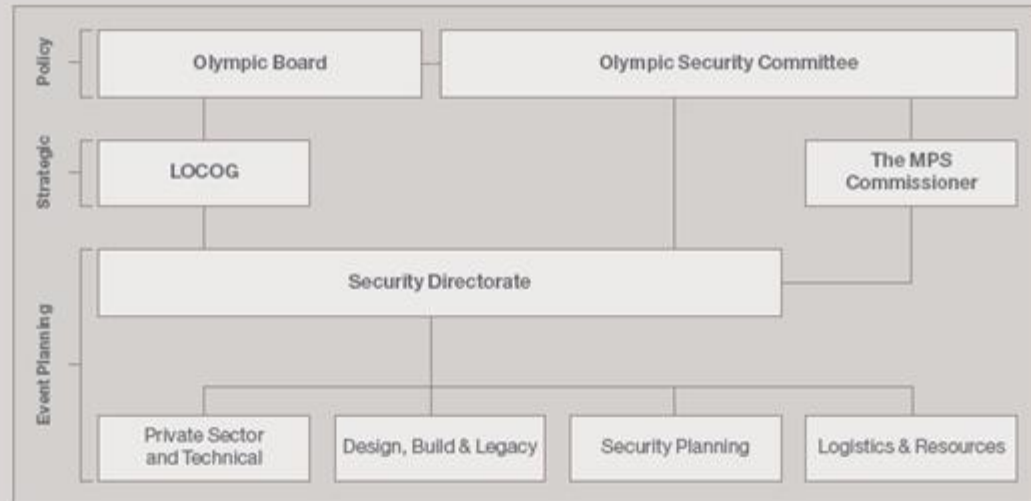
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

US Cybernotes 2003 – page 2

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
3Com ¹	Multiple	SuperStack 3 Firewall	SuperStack 3 Firewall Content Filter Bypassing	Medium	CyberNotes-2003-06
3Com ¹⁰	Multiple	SuperStack II RAS 1500	SuperStack II RAS 1500 Malicious IP Header Denial of Service & Inadequate Authentication	Low/Medium <i>(Medium if sensitive information can be obtained)</i>	CyberNotes-2003-07
3D-FTP ¹¹	Windows	3D-FTP Client 4.0	3D-FTP Client Buffer Overflow	High	CyberNotes-2003-09
3ware Software ¹²	Multiple	Disk Management Software 1.10.020, 1.10.012	Disk Management Denial of Service	Low	CyberNotes-2003-03
4D Inc. ¹³	Windows	WebSTAR 5.2-5.2.4, 5.3, 5.3.1	4D WebSTAR Remote Buffer Overflow	High	CyberNotes-2003-19
Abuse-SDL ¹⁴	Multiple	Abuse-SDL 0.7.0	Abuse-SDL Buffer Overflow	High	CyberNotes-2003-13
access_referrer. sourceforge.net ¹⁵	Unix	Apache mod_access_referrer 1.0.2	Apache Mod_Access_Referrer Remote Denial of Service	Low	CyberNotes-2003-08
access-remote- pc.com ¹⁶	Windows	Remote PC Access 2.2	Remote PC Access Denial of Service	Low	CyberNotes-2003-11
ACLogic ¹⁷	Multiple	CesazFTP	CesazFTP Remote Denial of Service		
Acme Laboratories ¹⁸ <i>SuSE issues advisory²⁰</i>	Unix	httpd 2.21b, 2.21, 2.22, 2.23b1	httpd defang() Remote Buffer Overflow CVE Name: CAN-2003-089		
Acme Laboratories ¹⁹ <i>Connectiva issues advisory²¹</i>	Unix	Acme mini httpd 1.0 1.1.0, 1.10-1.16, httpd 1.0, 1.90 a, 1.95, 2.0-2.23 b1	httpd/mini httpd Director Traversal CVE Name: CAN-2002-1562		
ActivCard Corporation ²⁴	Windows XP	ActivCard Gold 1.21, 2.2	ActivCard Gold Cached Static Password	Medium	CyberNotes-2003-08
Active PHP Bookmarks ²⁵	Multiple	Active PHP Bookmarks 1.1.01	Active PHP Bookmarks Multiple File Include	High	CyberNotes-2003-01
Adaltis Informatique ²⁶	Unix	D-Forum 1.0, 1.10, 1.11	D-Forum Remote File Include	High	CyberNotes-2003-04
Adiscon GmbH ²⁷	Windows	Monitor Ware Agent 1.3, 5.4.21 SP1, 5.0 beta	WinSyslog Interactive Syslog Server Long Message Remote Denial of Service	Low	CyberNotes-2003-22
Adiscon GmbH ²⁸	Windows	WinSyslog 4.21 SP1	WinSyslog Long Syslog Message Remote Denial of Service	Low	CyberNotes-2003-21
Adobe Systems Inc. ²⁹	Windows	SVG Viewer 3.0 & prior	SVG Viewer Alert Method Code Execution	High	CyberNotes-2003-21
Adobe Systems Inc. ³⁰	Unix	Acrobat Reader (UNIX) 5.05-5.0.7, 4.05	Adobe Unix Acrobat Reader Buffer Overflow	High	CyberNotes-2003-14
Adobe Systems Inc. ³¹	Windows	SVG Viewer 3.0 & prior	SVG Viewer 'postURL' & 'getURL' Restriction Bypass	Medium	CyberNotes-2003-21
Adobe Systems Inc. ³²	Windows	SVG Viewer 3.0 & prior	SVG Viewer Active Scripting Security Bypass	Medium	CyberNotes-2003-21
Adobe Systems, Inc. ³³	Windows	Acrobat 5.0, 5.0.5	Acrobat JavaScript Parsing Engine	High	CyberNotes-2003-10
Adobe Systems, Inc. ³⁴ <i>Upgrade available & exploit virus³⁵</i>	Windows: 95/98/NT 4.0/2000, XP, MacOS, Unix	Acrobat 4.0 5, 4.0 5c, 4.0, 4.0.5 a, 5.0, 5.0.5, Acrobat Reader 4.0 5, 4.0 5c, 4.0, 4.0.5 a, 5.0, 5.0.5	Acrobat Plug-in Digital Signature CVE Name: CAN-2002-005	High	CyberNotes-2003-07 CyberNotes-2003-09
Aegis Group ³⁶	Windows	FoxWeb 2.5	FoxWeb Remote Buffer Overflow	High	CyberNotes-2003-19
AIDA-X ³⁷	Multiple	Mini-Webserver 1.1	Mini-Webserver Information Disclosure	Medium	CyberNotes-2003-14
akpop3d ³⁸	Unix	akpop3d 0.4-0.6, 0.7-0.7.5	akpop3d Authentication Code	Medium	CyberNotes-2003-18
Alabanza ³⁹	Multiple	AlaCart 1.0	AlaCart Authentication Authentication Bypass	High	CyberNotes-2003-25

Page 2 of 190

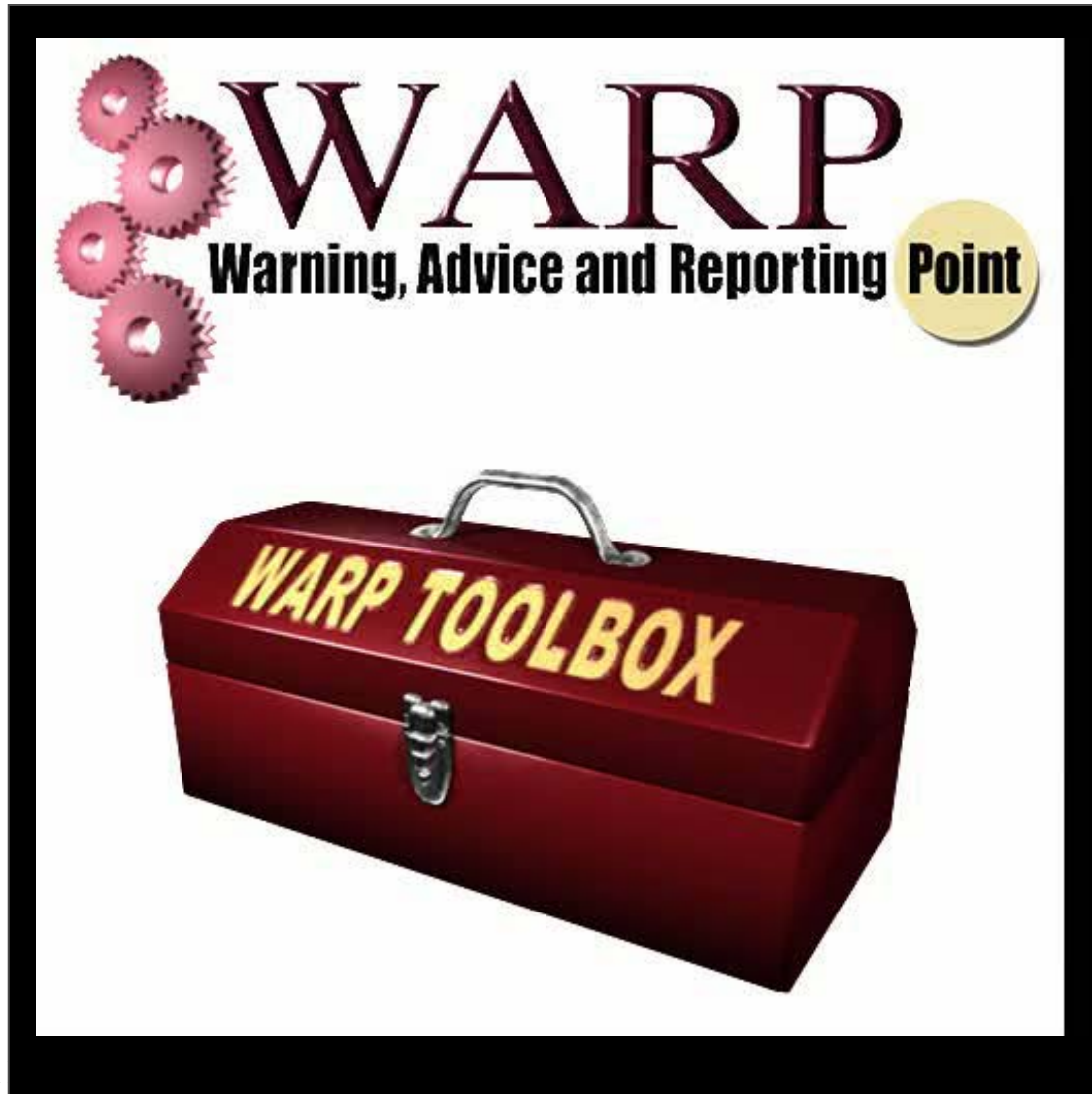
12.6a Security planning phase structure 2005–2008



12.6b Security implementation structure 2008–2012

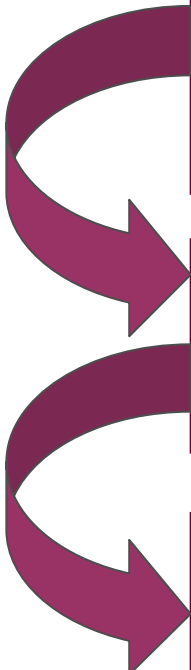


The WARP TOOLBOX



<http://www.warp.gov.uk>

WARPs – A development model



Stage 1: Show the benefits of the WARP to the community through tailored **warning** service, so that everyone feels they are getting a personalised and valuable service.

Stage 2: Develop trust through encouraging members to help each other by sharing best practice and giving **advice** to each other through WARP facilities.

Stage 3: Encourage members to report their experiences of otherwise embarrassing attacks or problems (anonymously if necessary, through the operator) within the WARP collective learning.

Setting up WARP(s) for the Olympics

- NISCC already engaged with Olympics but awareness low
- Need to identify a champion
- Need to identify community(s)
- The WARP Toolbox – www.warp.gov.uk
- Fits the right ethos
 - NfP, cooperative, collaborative
- [Filtered Warning Software]

A final thought

*“It is not from ourselves that we learn
to be better than we are”*

~Wendell Berry