OFFICE OF THE DIRECTOR
NATIONAL RESPONSE CENTRE FOR CYBER CRIMES (NR3C)
FEDERAL INVESTIGATION AGENCY HEADQUARTERS
ISLAMABAD

No. FIA/NR3C/Reports/DD-NS/2014/10/ Date: 12/02/2014

To,

The Director General,
Federal Investigation Agency(FIA),
HQs. Islamabad.

SUBJECT: CYBERSECURITY GUIDELINES FOR GOVERNMENT DEPARTMETNS

This is with reference to meeting held on Feb 3, 2014 in the office of Project Director NR3C. The task of preparation of written material, rules and guidelines for safe usage of Information Technology and Internet for Government Employees was assigned to NR3C Network Security and R&D team.

2. Cyber Security Guidelines for Government Employees/Departments, prepared by above mentioned teams are attached herewith please.

3. Submitted for your kind perusal and further necessary direction please.

Encl: (7)

(**Mohsin Hassan Butt) PSP**
Project Director NR3C

OFFICE OF THE PROJECT DIRECTOR
NATIONAL RESPONSE CENTRE FOR CYBER CRIMES (NR3C)
Federal Investigation Agency(FIA)
2nd Floor National Police Foundation Building
Sector G-10/4, ISLAMABAD
Phone: 051-9106380, Fax: 051-9106383

Cyber Security Guidelines for Government Departments and Employees

Version 0.1

EXECUTIVE SUMMARY

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, mobile networks, computer systems, handheld devices and embedded processors and controllers. Cyberspace encompasses critical information infrastructure, online banking systems, e-commerce, e-business, e-government and any service running over Internet. Cyberspace is such a powerful and influential domain that it is perceived as fifth space and has capability to transform national cultures into universal culture. The emergence of cyberspace generated new dimensions of legislative, political, diplomatic, informational, military and economic control, power and influence systems. Exploitation of vulnerabilities in cyberspace can cause grave damage to national security and can cripple down critical infrastructure of a nation.

Historical incidents in cyberspace like stuxnet and DDOS attack on Estonia has opened up the possibility of existential threat to a nation from cyber attacks. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and organization as well as user's assets.

National Response Centre for Cyber Crimes (NR3C) / FIA is receiving complaints regarding cyber crimes and cyber security incidents in Pakistan under enacted laws to deal with cyber crimes. It is global practice that Law Enforcement Agencies can not prevent cyber crimes by just taking punitive measures against cyber criminals. It demands holistic approach including awareness, best practices and guidelines specially for government institutions on safe use of Internet and protection of information systems including handheld devices.

Today, web browsers such as Internet Explorer, Mozilla Firefox, and Apple Safari (to name a few), are installed on almost all types of computing devices. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer which may result in data leakage, data loss, data theft, data hiding, data modification and data eraser by intruder or hacker.

Latest research reports reflect that 4.55 billion people worldwide are expected to use a mobile phone in 2014. The global smartphone audience surpassed the 1 billion mark in 2012 and will total 1.75 billion in 2014. Smartphones, or mobile phones with advanced capabilities like those of personal computers (PCs), and relatively lax security have made them attractive targets for attackers. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on personal computers. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a "botnet"). Malicious software can also send device information to attackers and perform other harmful commands. Mobile phones can also spread viruses to PCs that they are connected to. A compromised mobile device can provide a wealth of information to an attacker. The possible targets for attackers on Mobile Phones include but not limited to: SMS, Email, video/photo, social networking, location information, voice recording, documents and credentials.

Keeping in view the above threat landscape, current release of Cybersecurity Guideline for Government Departments and Employees, covers Web Browser Security and Mobile Phones Security. Mobile Phone Security guidelines encompass following types of mobile phones.

- Google Android based Phones
- Apple iOS based Phones.

Security guidelines for following popular web browsers are part of booklet.

- Microsoft Internet Explorer
- Mozilla Firefox
- Apple Safari

(**Mohsin Hassan Butt) PSP**

Project Director NR3C

Table of Contents

2. Threat Landscape for Mobile Devices:

A recent study commissioned by IT security solutions provider Lumension and conducted by the Ponemon Institute indicate that a large majority (75 percent) of IT security experts feel that attacks on smartphones and other mobile devices will be the main security concerns in the year 2014. A lack of consistency across security platforms was identified as a concern, particularly when it comes to defining malware. When examining more than 500,000 mobile applications for Android, HP said it found major discrepancies between how antivirus engines and mobile platform vendors defined and classified malware.

Just 46 per cent of mobile applications that were examined used encryption properly, and sandbox bypass vulnerabilities were the most prevalent and damaging for Java users. To reduce risk in this changing threat landscape, HP said both organizations and device users should stay aware of security pitfalls in frameworks. A combination of people, process and technology can minimize the attack surface.

3.1 Cyber Security Guidelines for Google Android Phones

Security Guideline	Rationale
Update firmware to latest version	Firmware updates often include critical security fixes that reduce the probability of an attacker exploiting the device.
Enable 'Password'	Requiring a password to unlock the device increases the effort required to use the device or access data stored on it.
Enable 'Require alphanumeric value'	Requiring an alphanumeric password to unlock the device increases the difficulty of determining the password by an attacker seeking unauthorized access.
Set 'timeout in minutes' for 'Sleep'	Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.
Remove Entries in 'Wi-Fi'	A trusted but unauthenticated Wi-Fi network may be spoofed and automatically joined if it is not forgotten after last use. Additionally, if such a network has a common SSID, such as "default" or "Linksys," it is probable that the device will encounter an untrusted instance of a same-named Wi-Fi network and automatically join it.
Disable 'Network Notification	Requiring the user to manually configure and join a Wi-Fi network reduces the risk of inadvertently joining a similarly named yet untrusted network (i.e. "default" vs. "default").
Disable 'Wi-Fi'	Disabling the Wi-Fi interface reduces the remote attack surface of the device. Additionally, at present, the cellular data network is a more difficult medium to sniff than Wi-Fi.
Disable 'Bluetooth'	If the user does not need Bluetooth enabled, it should be disabled to prevent discovery of and connection to supported Bluetooth services.
Disable 'Location Services'	Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means.
Enable 'Airplane Mode'	If the user enters an environment where signal transmission or reception are unnecessary then enabling Airplane Mode eliminates the remote attack surface of the device.
Erase all data before return, recycle, reassignment, or other disposition	Deleting data stored on the device before returning, recycling or disposing of the device reduces the probability of an attacker subsequently accessing confidential information previously stored on the device.
Disable 'Notifications'	If the device becomes lost or is unattended then disabling notifications reduces the capability of an attacker to obtain confidential information displayed on the screen.
Enable 'Lock SIM card'	On applicable phones, SIM cards often contain contact and other personal information. This setting will lock the SIM card so that it requires a PIN to access. Parties who do not know the SIM PIN should not be able to view the SIM card's contents, nor use the SIM card in another mobile device.
Disable 'make passwords visible'	Enforcing this control reduces the capability of an attacker to observe user input and learn the device password.

Enable 'Encrypt phone'	Once the phone is encrypted, a numeric PIN or password is required each time the phone is powered on, protecting personal data that would otherwise be easily recovered through a variety of methods. The phone cannot be unencrypted except by performing a factory data reset, which will erase all data on the phone.
Disable 'developer options'	Disabling command and data functions reduces the attack surface of the device. Since the same port is used to charge the phone, combined with the common availability in airports and other public places for phone charging, it is important to ensure that charging the phone does not open an attack vector.
Disable 'Unknown sources'	Disabling installation from untrusted distribution channels protects against inadvertent installation of untrusted or malicious applications.
Limit the 'number of messages' for 'Text message limit'	Limiting the number of messages saved on the device potentially reduces the scope of information disclosure in the event of device compromise.
Limit the 'number of messages' for 'Multimedia message limit'	Limiting the number of messages saved on the device potentially reduces the scope of information disclosure in the event of device compromise.
Browser Settings	This section provides guidance on the secure configuration of settings related to the built-in browser.
Disable 'JavaScript'	JavaScript lets web programmers control elements of the page, for example: a page that uses JavaScript process may process login credentials or cause a linked page to appear in a new pop-up page. JavaScript should only be enabled when browsing trusted sites.
Enable 'Show security warnings'	Enforcing this control reduces the probability that invalid certificates can be used to provide unauthorized access to confidential information or breach its integrity.
Disable 'Form auto-fill'	Enforcing this control reduces the probability of an attacker obtaining or using confidential information stored on the device such as names, credit card numbers and passwords.
Disable 'Accept Cookies'	Disabling 'Accept Cookies' reduces the probability of an attacker tracking, altering or stealing confidential information. HTTP cookies may contain user-specific data such as usernames, passwords and account numbers.
Enable 'Block pop-ups'	Enabling the Pop-up Blocker will block all pop-ups to guard a user against any attacks launched using pop-up windows.
Disable 'plug-ins'	Flash and other plug-ins let web programmers control elements of the page, for example: a page that uses Flash processing may process login credentials or cause a linked page to appear in a new pop-up page. Plug-ins should only be enabled when browsing trusted sites.
Disable 'Remember passwords'	Enforcing this control reduces the probability of an attacker obtaining or using passwords stored on the device.

3.2 Cyber Security Guidelines for Apple iOS based Phones

Security Guideline	Rationale
System Settings	This section provides guidance on the secure configuration of system settings.
Update firmware to latest version	Firmware updates often include critical security fixes that reduce the probability of an attacker exploiting the device.
Enable Passcode Lock	Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.
Disallow Simple Passcode	Permitting an alphanumeric password to be configured to unlock the device permits the user to increase the difficulty of determining the password by an attacker seeking unauthorized access.
Set Auto-lock	Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.
Enable Erase Data	This configuration item determines whether the device will automatically wipe its contents after excessive (10) failed passcode attempts. It is recommended that this feature be enabled. Excessive passcode failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.
Disable Passcode Unlock for Fingerprints	Disabling Passcode Unlock for Fingerprints can help avoid exposure to risk of unauthorized successful authentication via TouchID, by false positive or by intentional attacks (e.g., making use of latent fingerprints).
Disable Access to Control Center on Lock Screen	Disabling access to the Control Center on the Lock Screen can potentially mitigate future variations of iOS lock screen bypass exploits that may be possible for attacker who have gained physical access to the device.
Forget Wi-Fi networks to prevent automatic rejoin	A trusted but unauthenticated Wi-Fi network may be spoofed and automatically joined if it is not forgotten after last use. Additionally, if such a network has a common SSID, such as "default" or "linksys", it is probable that the iOS device will encounter an untrusted instance of a same-named Wi-Fi network and automatically attempt to join it.
Turn off Ask to Join Networks	Requiring the user to manually configure and join a Wi-Fi network reduces the risk of inadvertently joining a similarly named yet untrusted network.
Turn off Auto-Join for all Wi-Fi networks	Auto-Join may expose credentials at unexpected times and locations (e.g., if forms-based authentication occurs over unencrypted HTTP, or a spoofed SSID is encountered), and for Wi-Fi networks that require HTTP(S) forms authentication, this feature will cause credentials to persist on disk, potentially placing the confidentiality of the credentials at risk if physical custody of the device is lost.
Turn Off AirDrop	Turning off AirDrop discoverability prevents the device from making

Discoverability	itself discoverable to other devices for AirDrop functionality. It is recommended to restrict device discoverability when this functionality is not needed.
Turn off Wi-Fi when not needed	Disabling the Wi-Fi interface reduces the remote attack surface of the device.
Turn off VPN when not needed	If the device has a VPN connection configured, it should only be turned on when VPN access is required. If the VPN is left on, the user may not be mindful of the nature of the information they are transmitting on the network. Additionally, malicious or exploited iPhone applications may access VPN resources.
Turn off Bluetooth when not needed	Disabling Bluetooth when not needed reduces the remote attack surface of the device and prevents discovery of and connection to Bluetooth services.
Turn off Personal Hotspot when not needed	Disabling the Personal Hotspot makes the hotspot unavailable to unauthorized access attempts and reduces the overall remote attack surface of the device.
Turn off Location Services	Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means.
Turn on Airplane Mode	If the user enters an environment where no signal transmission or reception is intended, Airplane Mode can be turned on to ensure that the device does not initiate or respond to any signals. This reduces the remote attack surface.
Disable View in Lock Screen for apps when device is locked	Parties who do not know the passcode lock should not have read access to the notifications displayed by the device.
Enable Automatic Downloads of App Updates	App updates often include critical security fixes that reduce the probability of an attacker exploiting vulnerabilities in apps.
Enable Find My iPhone	This control enables the remote tracking, remote wiping, remote custom message display, and Activation Lock features of the iOS device.
Erase all data before return, recycle, reassignment, or other disposition	In normal operations, deleting data on an iOS device renders it inaccessible through the user interface but the data is not erased from the device. Erasing stored data by securely discarding the block storage encryption key before returning, recycling, disposing of, or otherwise placing a device out of the user's control reduces the probability of an attacker subsequently accessing confidential information previously stored on the device.
Safari Settings	This section provides guidance on the secure configuration of settings related to the Safari application (web browser) on the iOS mobile devices.
Disable JavaScript	JavaScript should only be enabled before browsing trusted sites.
Enable Fraudulent Website Warning	Enabling a warning can help you avoid accidently visiting some known phishing and other fraudulent sites covered by this feature.
Disable Auto Fill for Contact Information	Disabling AutoFill can help avoid the storage of sensitive information locally on the device, as well as reduces the likelihood of automated

	unauthorized use of information on a site in the event unauthorized access is gained to the device.
Disable Auto Fill for Credit Card Information	Disabling AutoFill can help avoid the storage of sensitive information locally on the device, as well as reduces the likelihood of automated unauthorized use of information on a site in the event unauthorized access is gained to the device.
Delete Saved Password Information	Deleting saved website credential information from the browser configuration helps prevent unauthorized access to such sensitive data in the event unauthorized access is gained to the device.
Delete Saved Credit Card Information	Deleting saved Credit Card information from the browser configuration helps prevent unauthorized access to such sensitive data in the event unauthorized access is gained to the device.
Turn On Private Browsing When Needed	Enabling Private Browsing can protect certain private information and block some websites from tracking browser activity.
Turn On Do Not Track	Enabling Do Not Track instructs the iOS 7 Safari browser to send an optional header in HTTP requests made from the app that indicates a preference not to be tracked by websites. This optional header is voluntary in nature, having no method to enforce adherence and providing no guarantee that web sites will honor the preference. However, a large number of websites do honor it so there is privacy benefit in enabling it.
iPhone Configuration Utility Settings	This section provides guidance on the secure configuration of iOS mobile devices with the iPhone Configuration Utility (iPCU), version 3.6.2.300. The iPhone Configuration Utility is a download available from Apple at http://www.apple.com/support/iphone/enterprise that lets users create, maintain, and sign configuration profiles, track and install provisioning profiles and authorized applications, and capture device information including console logs.
Set Security to disallow profile removal	Restricting the removal of a configuration profile is necessary to enforce the settings contained within the respective profile. If a user can circumvent profile requirements simply by uninstalling the profile, the continued enforcement of profile controls cannot be assured and intended device security is highly reduced.
Require passcode on device	Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.
Do Not Allow Simple Value	Simple passcodes such as those with repeating, ascending, or descending character sequences are easily guessed. Preventing the selection of passwords containing such sequences increases the complexity of the passcode and reduces the ease with which an attacker may attempt to guess the passcode in order to gain access to the device.
Require alphanumeric value	Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode and therefore the difficulty of determining the password by an attacker seeking unauthorized access.

Set minimum passcode length	Requiring at least five characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.
Set Minimum number of complex characters	Requiring at least one complex character increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.
Set Maximum Auto-lock	Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.
Set Maximum number of failed attempts	Excessive passcode failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.
Enable Prevent Move for Sensitive Mail Accounts	Permitting the movement of messages from one account to another intentionally or unintentionally can result in the exfiltration or loss of data from sensitive mail systems.
Require Use Only in Mail for Sensitive Mail Accounts	Permitting apps other than the Mail app to send messages from a mail account can limit an organization's ability to tightly control against the exfiltration or loss of sensitive data from an iOS device.

4. Threat Landscape for Web Browsers

Internet Explorer is a full featured web browser, developed by Microsoft Inc. in 1995 and it's included by default on computers with Microsoft's Windows operating system. It is one of the most widely used and popular web browsers currently. Internet Explorer was the one that had the most market share back in 2002 and 2003 (95% usage share). Internet Explorer is vulnerable and exploitable with default configurations. List of few relevant vulnerabilities are as under:-

- Microsoft Internet Explorer allows remote attackers to execute arbitrary code or cause a denial of service.
- Microsoft Internet Explorer 7 through 11 allows local users to bypass the Protected Mode protection mechanism, and consequently gain privileges, by leveraging the ability to execute sandboxed code.
- Microsoft Internet Explorer 8, and possibly other versions, detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https.

Firefox has been at the forefront of Web browser security, introducing numerous features that protect you from phishing schemes, viruses and other common exploits. The browser includes a powerful pop-up blocker and strong authentication protocols that prevent attackers from running unauthorized code when you are browsing. Although firefox is considered as most secure browser as compared to other popular browsers, However many vulnerabilities has been identified in Firefox, some of the most relevant are as under:-

- Local Java applets may read contents of local file system. An issue with Java applets where in some circumstances the applet could access files on the local system when loaded using the a file:/// URI and violate file origin policy due to interaction with the codebase parameter.
- A specifically named DLL file on a Windows computer is placed in the default downloads directory with the Firefox installer, the Firefox installer will load this DLL file when it is launched.
- Allow for cross-site scripting (XSS) attacks by exploiting default configuration of browser.

- The Mozilla Updater can be made to load a specific malicious DLL file from the local system. This DLL file can run in a privileged context through the Mozilla Maintenance Service's privileges, allowing for local privilege escalation.

The Safari Web Browser is developed by Apple Inc. and included with the Mac OS X and iOS operation systems. First released as a public beta on January 7, 2003 on the company's Mac OS X operating system. It became Apple's default browser beginning with Mac OS X v10.3. Latest version of Safari Browsers is v6.0.2. Following are relevant detected vulnerabilities in safari browser by CVE.

- Apple Safari allows remote attackers to execute arbitrary code or cause a denial of service via a crafted web site.
- Apple Safari allows remote attackers to bypass the Same Origin Policy and discover credentials by triggering auto fill of sub frame form fields.
- Apple Safari disables the Private Browsing feature upon a launch of the Web Inspector, which makes it easier for context-dependent attackers to obtain browsing information by leveraging Local Storage / files.

5.1 Cyber Security Guidelines for Microsoft Internet Explorer

Security Guideline	Rationale
Anti-Malware	This section provides guidance on the secure configuration of Anti-Malware functionality in Internet Explorer
Set 'Allow software to run or install even if the signature is invalid' to 'Disabled'	Microsoft ActiveX controls and file downloads often have digital signatures attached that certify the file's integrity and the identity of the signer (creator) of the software. Such signatures help ensure that unmodified software is downloaded and that you can positively identify the signer to determine whether you trust them enough to run their software. The validity of unsigned code cannot be ascertained.
Set 'Prevent Bypassing SmartScreen Filter Warnings' to 'Enabled'	If this setting is enabled and the SmartScreen Filter is active, the user can ignore a SmartScreen Filter warning and navigate to a site determined to be unsafe.
Set 'Prevent users from bypassing SmartScreen Filter's application reputation warnings about files that are not commonly downloaded from the Internet' to 'Enabled'	This setting is important from a security perspective because Microsoft has extensive data illustrating the positive impact the SmartScreen filter has had on reducing the risk of malware infection via visiting malicious websites.
Configure 'Do not allow users to enable or disable add-ons'	Users often choose to install add-ons that are not permitted by an organization's security policy. Such add-ons can pose a significant security and privacy risk to your network.
Set 'Disable Save this program to disk option' to 'Enabled'	Users could download and execute hostile code from Web sites.
Set 'Select SmartScreen Filter mode for Internet Explorer 9' to 'Enabled	This setting is important from a security perspective because Microsoft has extensive data illustrating the positive impact the SmartScreen filter has had on reducing the risk of malware infection via visiting malicious websites.
ActiveX Settings	
Set 'Disable Per-User Installation of ActiveX Controls' to 'Enabled'	Restricting the installation of ActiveX controls to administrators and using the ActiveX Installer Service or some other centralized software deployment tool is a more effective method for avoiding malware.
Set 'Only use the ActiveX Installer Service for installation of ActiveX Controls' to 'Enabled'	Installing ActiveX controls using the standard installation process is less secure than using the ActiveX Installer Service.
Set 'Turn off ActiveX opt-in prompt' to 'Disabled'	If the user were to enable this setting the ActiveX opt-in prompt would be disabled and malicious ActiveX controls could be executed without the user's knowledge.
Set 'Turn on ActiveX	ActiveX Filtering allows you to make an informed decision about

Filtering' to 'Enabled'	every ActiveX control you run by giving you the ability to block ActiveX controls for all sites, and then turn them on for only the sites that you trust. This can help improve your protection against risky and unreliable ActiveX controls.
Browsing History	
Configure 'Prevent Deleting Cookies'	If a user is suspected of visiting unauthorized website the information stored in the data cookies could be useful in verifying where he or she went online.
Configure 'Prevent Deleting Temporary Internet Files'	If a user is suspected of visiting unauthorized website the information stored in the Temporary Internet Files folder could be useful in verifying where he or she went online.
Configure 'Turn off "Delete Browsing History" functionality'	If users can delete their browsing history it will be easier for them to hide evidence if they have be visiting unauthorized sites.
Component Updates	
Configure 'Automatically check for Internet Explorer updates'.	If you enable this policy setting, Internet Explorer checks the Internet for a new version approximately every 30 days and prompts the user to download new versions when they are available. Newer versions might not comply to the Internet Explorer version requirements of your organization.
Certificates and Protocols	
Set 'Secure Protocol combinations' to 'Enabled: Only use TLS 1.0'	The allowed encryption protocols determines the possible encryption types that can be used. Preventing the use of older protocols decreases vulnerability.
Set 'Check for signatures on downloaded programs' to 'Enabled'	Although digitally signing software does not guarantee that it includes no malware, it does reduce the risk and it provides another potential path of investigation should the software include a dangerous payload.
Internet Communication Management	
Set 'Disable Browser Geolocation' to 'Enabled'	This setting has a small impact on user privacy because users may unknowingly allow their browser to share location data with web sites that they visit. The value of enabling this setting is diminished due to the fact that malicious web sites can learn a great deal about the location of a user merely by analyzing their IP address.
Internet Explorer Process Security Features	
Set 'Restrict File Download' to 'Enabled'	In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on a user's hard disk drive if they

	click the wrong button and accept the download.
Set 'Restrict ActiveX Install' to 'Enabled'	Users often choose to install software such as ActiveX controls that are not permitted by their organization's security policy. Such software can pose significant security and privacy risks to networks.
Set 'Consistent Mime Handling' to 'Enabled'	MIME file type spoofing is a potential threat to your organization. You should ensure that these files are consistent and properly labeled to help prevent malicious file downloads that may infect your network. Note This policy setting works in conjunction with, but does not replace, the MIME Sniffing Safety Features settings.
Set 'Protection From Zone Elevation' to 'Enabled'	These restrictions depend on the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, malicious Web pages may attempt to elevate themselves from their current zone into another zone with higher privileges.
Set 'Scripted Window Security Restrictions' to 'Enabled'	The Internet Explorer Processes (Scripted Window Security Restrictions) setting restricts pop-up windows and does not allow scripts to display windows in which the title and status bars are not visible to the user or that hide other windows' title and status bars. When enabled, this policy setting help make it difficult for malicious Web sites to control your Internet Explorer windows or fool users into clicking the wrong window.
Internet Zone	
Set 'Allow drag and drop or copy and paste files' to 'Enabled:Disable	Content hosted on sites located in the Restricted Sites Zone are more likely to contain malicious payloads and therefore this feature should be blocked for this zone.
Set 'Allow font downloads' to 'Enabled:Disable'	It is possible that a font could include malformed data that would cause Internet Explorer to crash when it attempts to load and render the font.
Set 'Allow paste operations via script' to 'Enabled:Disable'	A malicious script could use the clipboard in an undesirable manner, for example, if the user had recently copied confidential information to the clipboard while editing a document a malicious script could harvest that information. It might be possible to exploit other vulnerabilities in order to send the harvested data to the attacker.
Require alphanumeric value	Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode and therefore the difficulty of determining the password by an attacker seeking unauthorized access.
Set 'Allow script-initiated windows without size or position constraints' to 'Enabled:Disable'	If you enable this policy setting, scripts will be able to launch and resize additional browser windows without and limits on size or position, attackers have used this feature in the past to confuse users and cause them to click on links that led to undesirable consequences.
Set 'Automatic prompting for file downloads' to	Users may accept downloads that they did not request, those downloaded files may include malicious code.

'Enabled:Disable'	
Set 'Download unsigned ActiveX controls' to 'Enabled:Disable'	Unsigned code is potentially harmful, especially when coming from an untrusted zone.
Set 'Initialize and script ActiveX controls not marked as safe' to 'Enabled:Disable'	This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. This increases the risk of malicious code being loaded and executed by the browser.
Set 'Logon options' to 'Enabled:Prompt for user name and password'	Users could submit credentials to servers operated by malicious people who could then attempt to connect to legitimate servers with those captured credentials.
Set 'Only allow approved domains to use ActiveX controls without prompt' to 'Enabled:Enable'	If the user were to disable the setting for the zone, malicious ActiveX controls could be executed without the user's knowledge.
Set 'Software channel permissions' to 'Enabled:High safety'	Any setting lower than High Safety could cause a user to install software that includes malicious code.
Set 'Use Pop-up Blocker' to 'Enabled:Enable'	Pop-up windows have been used on web sites that host malicious content to trick users into clicking on dangerous links or to confuse users by hiding elements of the browser interface.
Set 'Scriptlets' to 'Enabled:Disable'	Scriptlets have been exploited by malicious users in the past, one example is the malware Exploit-MSWord.k which embedded the class ID of the Microsoft Scriptlet Component within a Word document and the URL of a website that hosted additional malicious software. When opened Microsoft Word would process the embedded object then download and activate the malicious payload. This particular vulnerability was patched several years ago but disabling this setting in untrusted zones helps mitigate against the entire class of attacks.
Set 'Automatic prompting for file downloads' to 'Enabled:Disable'	Users may accept downloads that they did not request, those downloaded files may include malicious code.
Set 'Logon options' to 'Enabled:Anonymous logon'	Users could submit credentials to servers operated by malicious people who could then attempt to connect to legitimate servers with those captured credentials.

5.2 Cyber Security Guidelines for Mozilla Firefox

Security Guideline	Rationale
Enable Auto Update	Security updates are critical in ensuring that a user a safe is from known vulnerabilities. Therefore, automatic checking of updates should be enabled.
Enable Auto Notification of Outdated Plugins	Outdated Plugins can be vulnerable or unstable which can be exploited by malicious websites. It is recommended to enable this feature so that users are notified and directed to update plugins.
Enable Information Bar for Outdated Plugins	Outdated Plugins can be vulnerable or unstable which can be exploited by malicious websites. It is recommended to enable this feature so that users are notified and directed to update Plugins.
Encryption Settings	
Enable SSL 3.0 and TLS 1.0	Enabling these protocols will allow Firefox to enforce selection of higher SSL and TLS encryption key lengths and more robust protocols.
Enable Warning of Loading Mixed Content	Enabling this setting will alert a user when some content on a secure communication channel is coming under a non secure channel. For example an SSL website can request part of content on a page under a non-SSL session. This can leave users vulnerable to eavesdropping and Man in the Middle attacks.
Enable Warning of Using Weak Encryption	This will protect users from the compromise of their data due to weak encryption.
Enable Online Certificate Status Protocol	To provide assurance on the validity of encryption Certificates these option should be enabled.
Dynamic Content Settings	
Disable Closing of Windows via Scripts	Preventing an arbitrary web site from closing the browser window will reduce the probability of a user losing work or state being performed in another tab within the same window.
Disable Downloading on Desktop	This will protect from downloading content on desktop and tricking users into running malicious binaries.
Enable Virus Scanning for Downloads	This will ensure that a downloaded file is scanned for viruses before the user has an opportunity to interact with the download.
Block Reported Web Forgeries	Enabling this feature will decrease the probability of a user falling victim to a phishing attack or unknowingly disclosing sensitive information to an untrusted party.
Block Reported Attack	Enabling this feature will decrease the probability of a user s browser

Sites	or system being exploited by known malware.
Disable Displaying Javascript in History URLs	Various browser elements, even a simple link, can embed javascript: URLs and access the javascript: protocol. The JavaScript statement used in a javascript: URL can be used to encapsulate a specially crafted URL that performs a malicious function.
Block Pop-up Windows	By enabling the Pop-up blocker all Pop-ups will be blocked which will guard a user against any attacks launched using a Pop-up.
Network Settings	
Enable SSPI Authentication.	This will protect users from using weaker authentication.
Disable Referer from an SSL Website	It is possible that the URL of the SSL-protected, referring site contains sensitive information. By preventing Firefox from sending this URL, via an HTTP Referer header, to sites referred to by the SSL protected site an avenue for information disclose is eliminated.
Disable Sending LM Hash	The LM Hashing algorithm contains weaknesses that can be exploited to derive plain text authentication credentials.
Privacy Settings	
Accept Only 1st Party Cookies	These cookies are typically used to uniquely identify a user s session on a website. However, these cookies can be used by third party sites and malicious sites to track a user s activity on the web. Also, they can be used to store sensitive personally identifiable information. Cookie settings should be configured such that malicious websites cannot set the cookies.
Disallow Credential Storage	Credentials can be compromised if the computer is shared with other users. This setting will ensure that the passwords are not stored for websites.
Disable Prompting for Credential Storage	This setting will ensure that Firefox does not prompt for storing passwords which will be stored by Firefox. Stored credentials/sensitive data pose a risk as they can be compromised by malicious websites using information leakage bugs/advisories in Firefox.
Delete History and Form Data	If Firefox or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.
Delete Download History	If Firefox or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.
Delete Search and Form History	If Firefox or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.
Clear SSL Form Session Data	If Firefox or other applications executing at equal or higher contexts is compromised, potentially sensitive, persisted, form data is at increased risk.
Disable Caching of SSL Pages	This will protect user's confidential information from unauthorized disclosure.

Applications Settings	
Secure Application Plug-ins	Some malicious websites can have active content to exploit vulnerabilities in active content handling application plug-in. It is recommended as a defense-in-depth to always prompt when a website is about to load active content which is not trusted.
Disabling Auto-Install of Add-Ons	Add-Ons are extensions of the browser that add new functionality to Firefox or change its appearance. These run in a user s session allowing them do manipulate data and the behavior of the way Firefox interacts with other application and user commands. If malicious Add-Ons are installed automatically, a user's security could be completely compromised.

5.3 Cyber Security Guidelines for Apple Safari

Security Guideline	Rationale
Enable Pop-Up Blocker	By enabling the Pop-Up Blocker, all pop-ups will be blocked which will guard a user against any attacks launched using a pop-up.
Validate Proxy Settings	Given a proxy server's position between the web browser and web server, it has the ability to read and alter all information that is not cryptographically protected. Given this, if an untrusted proxy server is configured in Safari, the information sent and received by Safari is at considerable risk.
Accept only 1st Party Cookies	Configuring Safari to accept only 1st party cookies will limit the means by which an advertisement agency can build a browsing profile for the user.
Prompt for Insecure Form Submissions	Warning the user before form data is sent over an insecure transport provides the user with the opportunity to approve or deny the request based on the data's security classification.
Disable Storage and Usage of Form Data	If Safari or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.
Disable Storage and Usage of Credentials	If Safari or another application executing at an equal or higher security context is compromised, persisted authentication credentials are at increased risk.
Disable Storage and Usage of Address Book Card	If Safari or another application executing at an equal or higher security context is compromised, persisted personal and business contact information are at increased risk.
Enable Safe Browsing	Users will be alerted about known malicious web sites, thus decreasing the probability of a user's browser or system being exploited by known malware or phishing site.
Disable plug-ins	Plug-ins increase the remote attack surface of Safari. Additionally, some plug-ins do not undergo rigorous security testing and are

	therefore more likely to contain exploitable defects.
Disable Java	Some malicious websites can have active content to exploit vulnerabilities using Java. It is recommended as a defense-in-depth strategy to always disable unwanted features, such as Java.
Disable JavaScript	JavaScript continues to be an attack vector for exploiting vulnerabilities in the browser. Additionally, JavaScript is commonly leveraged by exploit authors to create a deterministic memory layout in support of increasing the reliability of exploits.
Use of Private Browsing	Safari provides private browsing for users who want to remove all traces of a session after a browsing session ends. This is particularly useful when using shared computers.

6. Additional Information

Security guidelines or controls mentioned in above tables are technical in nature and some of the controls implementation require assistance from network administrator or system administrator or equivalent technical resource. Additional Information on procedural details of any specific configuration guideline may be requested at pd@nr3c.gov.pk with copy to makram@nr3c.gov.pk. Request for Training or Seminar or Workshop on above mentioned cyber security controls may be sent at pd@nr3c.gov.pk or in the form of Letter addressed to Project Director National Response Centre for Cyber Crimes(NR3C), Federal Investigation Agency (FIA) Islamabad.

7. Concluding Remarks

Cyber Security guidelines for Government Departments and Employees is based upon practices followed by Law Enforcement Agencies(LEA) globally to minimize cyber crimes through enhanced cyber security awareness. Threats related to Mobile phones and Web Browsers have been presented to highlight the gravity and impact of risks associate with these tools and interfaces of modern electronic communication. Rationality of each security guideline or technical control further sheds light on severity of problem while we interact in cyber space. Cyber Security guidelines are implementable and configurable specific controls to minimize risks associated with cyber space. Implementation of controls mentioned in this booklet will improve security posture of individual and department upto up to the standard level.

Muhammad Akram Mughal,
Deputy Director Network Security NR3C/FIA

NR3C