Software Inspection and Authorization for the Research Preserve

The project will formally establish a change management structure that includes a thorough review process for the Secure Research environment. In the meantime, we propose the following guidelines for vetting software that is to be installed in the environment.

Responsible Parties

The research team and/or their IT support team are responsible for ensuring the actions and guidelines provided in this document are implemented.

Required Documentation

You must log into The RC website and complete the Software Request Form to request a new piece of software be added to your subscription.

Required Review

For software reviewed by ICT and provided by the University (e.g., Matlab, Mathmatica, etc.):

1. Please see the OIT Software Catalog for details on software that has been reviewed by ICT.
2. Prior to installation, complete the Software Vetting form found on the RC website for formal review and approval.

For software not provided by campus OIT:

1. Authorship of or development contributions to software must be checked against the banned list. If a contribution from any member of the attached excluded company list in **Appendix 1 –Excluded Companies** is present, the software cannot be used in the environment.
2. Prior to installation, complete the Software Vetting form found on the RC website for formal review and approval.

For Self-written software code:

Self-written software code shall follow the following guidance:

1. Secure coding principles are considered during development.

a. OWASP is a great reference for best practices, including:
    1. https://owasp.org/www-project-web-security-testing-guide/
    2. https://owasp.org/www-project-top-ten/
    3. https://owasp.org/www-project-dependency-track/

For Linux installations (libraries, etc.)

1. For Linux, ensure the package includes SELinux features.
2. Participate in the RedHat (or your distribution of Linux) project community for the latest news on updates and vulnerabilities, etc.
3. Install the latest versions of the application and/or library.
4. Consider if the library is one that is installed with the base package, or a new untested library. If untested, steps should be taken to verify the security of the code prior to installation. See guidance on Open-Source Software below in section 6.
5. Try to use libraries that are popular, widely used and have strong community support.
6. If possible, verify the origin and lineage of the code and associated libraries.
7. Check for records as to the identity of individual contributors.
8. Install signed packages from well-known repositories.

Additional Guidance for any Open-Source Software review and guidance

1. Know the type of licensing associated with the software. Is the source code released and open to the public or kept secret by the developer? Code kept secret can make it difficult to track changes to the code or verify security of the code.
2. Adopt strict coding standards and guidelines including at a minimum, the guidelines below.

    a. Manual auditing via regular code reviews or penetration testing by a human. This is especially important when code is used to access critical resources. Scanners can be used in addition, but they are limited to the vulnerability definitions included in the tool.
    b. Vulnerability scanning of the code (Veracode, etc.) • Can you verify the reliability and security of the code?
        i. NVD (National Vulnerability Database) NIST- Search known CVEs https://nvd.nist.gov/
        ii. CVE (Common Vulnerabilities and Exposures) details https://www.cvedetails.com/
    c. Have a process in place to monitor for vulnerabilities and to apply fixes/updates.
    d. Become a member of the specific projects open-source software community and monitor the site for new information on the open-source software.
        i. There should be widespread availability and use of the software, which increases the likelihood of detection for vulnerabilities.
        ii. Vulnerabilities should be immediately addressed as they are discovered by the community.
    e. Monitor/locate, review, and test software updates in sandbox prior to install on production systems.
    f. Integrate fixes into releases often
        i. If updates are on an irregular basis, they should be applied quickly, and be constantly addressed.

*Note: **Appendix 2 – Excerpts from NIST SP800-171B** is included as a reference to those controls called out in NIST SP800-171r2 which cover software management and vetting.*

Appendix 1 – Excluded Companies

Software shall not include services or products produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain. That includes the following entities, as well as their parents, affiliates, and subsidiaries.

Huawei Technologies Company

- Amartus, SDN Software Technology and Team
- Beijing Huawei Digital Technologies, Co. Ltd.
- Caliopa NV
- Centre for Integrated Photonics Ltd.
- Chinasoft International Technology Services Ltd.
- FutureWei Technologies, Inc.
- HexaTier Ltd.
- HiSilicon Optoelectronics Co., Ltd.
- Huawei Device Co., Ltd.
- Huawei Device (Dongguan) Co., Ltd.
- Huawei Device (Hong Kong) Co., Ltd.
- Huawei Enterprise USA, Inc.
- Huawei Global Finance (UK) Ltd.
- Huawei International Co. Ltd.
- Huawei Machine Co., Ltd.
- Huawei Marine
- Huawei North America
- Huawei Software Technologies, Co., Ltd.
- Huawei Symantec Technologies Co., Ltd.
- Huawei Tech Investment Co., Ltd.
- Huawei Technical Service Co. Ltd.
- Huawei Technologies Cooperative U.A.
- Huawei Technologies Germany GmbH
- Huawei Technologies Japan K.K.
- Huawei Technologies South Africa Pty Ltd.
- Huawei Technologies (Thailand) Co.
- iSoftStone Technology Service Co., Ltd.
- JV “Broadband Solutions” LLC
- M4S N.V.
- Proven Honor Capital Limited
- PT Huawei Tech Investment
- Shanghai Huawei Technologies Co., Ltd.
- TD Tech
- Tianwen Digital Media Technology (Beijing) Co., Ltd.
- Toga Networks Ltd

ZTE Corporation

- Anhui Wantong Information Systems Integration Company, Limited
- Bestel Communications Ltd.
- CASIC Shenzhen (Group) Company, Limited
- Chengdu Zhongxing Software Company, Limited
- Chengdu ZTE Software Company Limited
- Enablence Technologies Inc.
- Guangdong New Pivot Technology & Service Company Limited
- Hengyang ICT Real Estate Co., Ltd.
- Huanggang Education Valley Investment Holdings Co., Ltd.
- Intlive Technologies (Private) Ltd.
- Jiaxing Xinghe Capital Management Company Limited
- Kaznurtel LLC
- Kron Telekomunikasyon Hizmetleri A.S.
- Laxense, Inc.
- Nanjing Piaoxun Network Technology Co., Ltd.
- Nationz Technologies, Inc.New Idea Investment Pte. Ltd.
- Ningbo Zhongxing Technology Co., Ltd. Yunxiang
- Nubia Technology Ltd.
- OOO ZTE Russia Co., Limited
- Pengzhong Xingsheng
- Pt ZTE Indonesia
- Puxing Mobil Tech Company Ltd.
- S.C. First Project SA
- Shanghai Xingfei Science And Technology Company, Limited
- Shanghai Zhongxing Communication Co., Ltd.
- Shanghai Zhongxing Qunli Information Technology Ltd.
- Shanghai Zhongxing Telecom Equipment Technology & Service Company Limited
- Shanghai Zte Technologies Co., Ltd.
- Shenzhen Capital Group Co., Ltd.
- Shenzhen Changfei Investment Company Limited
- Shenzhen Force Science And Technology Co., Ltd.
- Shenzhen Smart Electronics Ltd.
- Shenzhen Weigao Semi-Conductor Technology Co., Ltd.
- Shenzhen Zhongxing Hetai Hotel Investment and Management Co., Ltd.
- Shenzhen Zhongxing ICT Company Limited
- Shenzhen Zhongxing Microelectronic Technology Company Limited
- Shenzhen Zhongxing Software Co., Ltd.

- Shenzhen Zhongxing Telecom Technology & Services Co., Ltd.
- Shenzhen Zhongxing Xinyu FPC Company Limited
- Shenzhen ZTE Kangxun Telecom Co., Ltd.
- Shenzen ZTE Hetai Hotel Investment Management Ltd.
- Sizhuo Zhongxing Hangzhou Technology Ltd.
- Telecom Innovations
- Wuxi Kaier Technology Co., Ltd.
- Wuxi Taclink Optoelectronics Technology
- Wuxi Zhongxing Optoelectronics Technologies Company Limited
- Xi'an Zhongxing New Software Company Limited
- Xian Zte Jingcheng Communication Company, Limited
- Xingtian Communication Technology Tianjin Co., Ltd.
- Yangzhou Zhongxing Mobile Telecom Equipment Co. Ltd.
- Zhongxing Software Company Limited
- Zhuhai Guangtong Automobile Co., Ltd
- ZTE 9 (Wuxi) Co., Ltd.
- Zte (Australia) Pty Ltd.
- Zte Canada Inc.
- ZTE Cooperatief U.A.
- ZTE Corporation South Africa (PTY) Limited
- Zte Czech, S.R.O.
- ZTE Do Brasil Ltda.
- ZTE Energy Co., Ltd.
- ZTE Energy (Tianjin) Company Limited
- ZTE France SASU
- ZTE Ghana Limited
- Zte Group
- ZTE Group Finance Co., Ltd.
- ZTE (Hangzhou) Company Limited
- ZTE (Hong Kong) Ltd.
- Zte Hrvatska D.O.O.
- ZTE India R&D Center Private Limited
- ZTE International Investment Co., Ltd.
- ZTE Italy, S.r.l.ZTE Kangxun Telecom Company Limited
- ZTE Malaysia Corporation SDN. BHD.
- ZTE Mauritius Ltd.
- ZTE Microelectronics Technology Co., Ltd.
- ZTE Mobile Tech Company Limited
- ZTE Netherlands B.V.
- Zte Nigeria Investment LTD.
- Zte Norway As
- Zte Portugal Projectos De Telecommunicacoes, Unipessoal, Lda
- Zte Romania Srl
- ZTE Service Deutschland GmbH
- Zte Singapore Pte. Ltd.
- ZTE Software Technology (Nanchang) Co.
- ZTEsoft Technology Company Limited
- ZTE Supply Chain Co., Ltd
- ZTE Sweden Ab
- ZTE Technology & Service Company Limited
- ZTE Telecom India Private Limited Company Limited
- ZTE (Thailand) CO., Ltd
- ZTE Ukraine LLC
- ZTE (USA) Inc.

Currently identified subsidiaries/affiliates of Hytera Communications Corporation, Hangzhou Technology Company, or Dahua Technology Company Dahua Technology Company

- Dahua Europe B.V.
- Dahua India
- Dahua Technology Australia PTY LTD
- Dahua Technology Brasil Participacoes LTDA
- Dahua Technology Colombia S A S
- Dahua Technology (Hong Kong) Co., Ltd.
- Dahua Technology Mexico S.A. de C.V.
- Dahua Technology Middle East FZE
- Dahua Technology Peru S.A.C.
- Dahua Technology Poland
- Dahua Technology Rus, LLC
- Dahua Technology Singapore PTE. LTD.
- Dahua Technology South Africa Proprietary Limited
- Dahua Technology USA Inc.
- DH Chile SpA
- Hangzhou Huacheng Network (or Internet) Technology Co., Ltd.
- Hangzhou Tanmu Technology Co., Ltd.
- Hangzhou Tecomore Technology Co., Ltd.
- Hangzhou Xiaohua Technology Co., Ltd.
- Guangxi Dahua Information Technology Co., Ltd.
- Guangxi Dahua Security Service Co., Ltd.
- Guangxi Dahua Video Technology Co., Ltd.
- Guangxi Dahua Zhicheng Co., Ltd.
- Guangxi Dahua Zongzhi Technology Co., Ltd.
- Shanxi Dahua Tianrun Technology Co., Ltd.
- Wuxi Dahua Ruide (or Ryder) Electronic Technology Co., Ltd.
- Zhejiang Dahua Anfang Internet Operation Service Co., Ltd.
- Zhejiang Dahua Chi Network Technology Ltd.
- Zhejiang Dahua Investment Management Co., Ltd.
- Zhejiang Dahua Juan Technology Co., Ltd.
- Zhejiang Dahua Network Operations Security Services Co., Ltd.
- Zhejiang Dahua Science and Technology Co., Ltd.

- Zhejiang Dahua Security Service Co., Ltd.
- Zhejiang Dahua System Engineering Co., Ltd.
- Zhejiang Dahua Technology Co., Ltd.
- Zhejiang Dahua Zhilian Co., Ltd.
- Zhejiang Hongrui Communication Technology Co., Ltd.
- Zhejian HuaRay Technology Co., Ltd.
- Zhejiang Huarui Science and Technology Co., Ltd. (listed as pending)
- Zhejiang Huatu Weixin Technology Co., Ltd.

Hangzhou Hikvision Digital Technology Company

- Beijing Bangnuo Storage Technology Co., Ltd.
- Beijing Hikvision Security Technical Services Ltd.
- CETC Finance Co., Ltd. (listed as pending)
- Chongqing Haikang Technology Co., Ltd.
- Chongqing Haikang Weishi System Technology Ltd.
- Chongqing Hikvision System Technology Co., Ltd.
- Cooperative Hikvision Europea U.A.
- Ezviv
- Fuyang HaiKang Baotai Security Technology Services Ltd.
- Hikvision Australia
- Hikvision Canada
- Hikvision do Brasil Comecio de Equipamentos de Seguranca
- Hikvision Europe
- Hikvision France
- Hikvision FZE
- Hikvision Korea
- Hikvision International
- Hikvision Italy
- Hikvision Poland
- Hikvision Singapore
- Hikvision South Africa
- Hikvision Spain
- Hikvision UK
- Hikvision USA
- Hangzhou Ezviz Network Co., Ltd.
- Hangzhou Haikang Weishi Technology Co., Ltd.
- Hangzhou Hikrobot Technology Co., Ltd. (listed as pending)
- Hangzhou Hikvision Security Equipment Leasing Services Ltd.
- Hangzhou Hikvision System Technology Ltd. (listed as pending)
- HDT International
- OOO Hikvision
- Prama Hikvision India Private Limited
- Secure Holdings Limited
- Shanghai Gaodwei Intelligence Traffic System Ltd.
- Wuhan Hikvision System Technology Co., Ltd.
- ZAO Hikvision

Hytera Communications Corporation

- Dongguan Hytera Communications Co., Ltd.
- Harbin Hytera Technology Ltd.
- Hebi Tianhai Electronic Information System Co., Ltd.
- Hebi Xinyuan Electronic Co., Ltd. (listed as indirect subsidiary)
- HYT
- HYT North America, Inc.
- Hytera America, Inc.
- Hytera Mobilfunk GmbH
- Hytera Communications (Australia) Pty Ltd
- Hytera Communications (Hong Kong) Company Limited
- Hytera Communications (UK) Co., Ltd.
- Hytera Comunicacoes do Brasil Ltda
- Hytera Mobilfunk GmbH
- Hytera Project Corp.
- Hytera Technology (Hong Kong) Company Limited
- Nanjing Hytera Software Technology Co., Ltd.
- Nanjing Zhouda Communications Technology Co., Ltd.
- Norsat International Inc.
- Sepura plc
- Shenzhen Anzhijie Science & Technology Co., Ltd.
- Shenzhen Haitianlang Science & Technology Co., Ltd.
- Shenzhen Hytera Communications Co., Ltd.
- Shenzhen Hytera Financial Leasing Co., Ltd.
- Shenzhen Hytera Technology Services Co., Ltd.
- Shenzhen Sea Technology Co., Ltd. tannoy
- Shenzhen SEG Communication Co., Ltd.
- Shenzhen Yunliantong Communication Service Co., Ltd.
- Sinclair
- Teltronic
- Tianjin Hytera Information Technology Co., Ltd.

1. If unsure, supplier status can be verified by consulting any of the following:
   https://sam.gov/SAM/pages/public/exclusionSearch/exclusionsView.jsf

2. https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2599-85-fr-52898/file
3. https://www.sam.gov/SAM/
4. https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=9ae4a21068f2bd41d4a5aee843b63ef1&ty=HTML&h=L&n=15y2.1.3.4.28&r=PART#ap15.2.744_122.4
5. https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file
6. https://www.bis.doc.gov/index.php/2011-09-12-20-18-59/export-and-reexport-faqs/cat/33-entity-list-faqs#faq_106

Appendix 2 – Excerpts from NIST SP800-171B

The excerpts in this Appendix are for reference to the applicable controls for software control and vetting required by NIST SP800-171r2.

3.4.8	**SECURITY REQUIREMENT** Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.8[a] *a policy specifying whether whitelisting or blacklisting is to be implemented is specified.*
	3.4.8[b] *the software allowed to execute under whitelisting or denied use under blacklisting is specified.*
	3.4.8[c] *whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing least functionality in the system; system security plan; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs not authorized to execute on the system; list of software programs authorized to execute on the system; security configuration checklists; review and update records associated with list of authorized or unauthorized software programs; change control records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for identifying software authorized or not authorized to execute on the system; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational process for identifying, reviewing, and updating programs authorized or not authorized to execute on the system; process for implementing blacklisting or whitelisting; mechanisms supporting or implementing blacklisting or whitelisting].

3.4.9	**SECURITY REQUIREMENT** Control and monitor user-installed software.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.9[a] *a policy for controlling the installation of software by users is established.*
	3.4.9[b] *installation of software by users is controlled based on the established policy.*
	3.4.9[c] *installation of software by users is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing user installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user-installed software; system monitoring records; system audit logs and records; continuous monitoring strategy; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for governing user-installed software; personnel operating, using, or maintaining the system; personnel monitoring compliance with user-installed software policy; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes governing user-installed software on the system; mechanisms enforcing rules or methods for governing the installation of software by users; mechanisms monitoring policy compliance].

3.7.4	**SECURITY REQUIREMENT** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	ASSESSMENT OBJECTIVE *Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].