

# A list of ENISA's 2014 work programme publications

The following table presents links to the ENISA Work Programme 2014 deliverables

|  | Deliverable   | Status   |
|--|---|--|
| <b>WS 1 – Support EU Policy Building</b>                                       |   |  |
| <b>WPK 1.1 – Identifying technological evolution, risks and challenges</b>     |   |  |
| D1   | Annual EU CyberSecurity Threats Landscape   | “ENISA Threat Landscape 2014”<br>Publication expected by 18.12.2014.<br><a href="https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2014">https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2014</a>  |
| D2   | Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors)  | 1) “Threat Landscape and good practice guide for smart home and converged media”<br>Publication expected by 18.12.2014.<br><a href="https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/threat-landscape-for-smart-home-and-media-convergence/">https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/threat-landscape-for-smart-home-and-media-convergence/</a><br>2) “Threat Landscape and good practice guide for internet infrastructures”<br>Publication expected by 15.12.2014.<br><a href="https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl">https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl</a> |
| <b>WPK 1.2 – Contributing to EU policy initiatives</b>                         |   |  |
| D1   | Engaging Cloud Computing Stakeholders in the EU's Cloud Computing Strategy and Partnership (workshops, contributions to Commission's SIG and ECP work, Q2-Q4 2014)  | ENISA, together with Cloud Security Alliance (CSA) and Fraunhofer-FOKUS, organised SecureCloud, a European conference with a specific focus on cloud computing security, on 1-2.04.2014.<br>Contributions EU Cloud Strategy (WG Certification, WG SLAs).   |
| D2   | Engaging with stakeholders for the secure implementation of EU's Smart Grids policies (workshops, contributions to COM' EG 2 and MS actions, Q2-Q4 2014)  | Dissemination workshop for the EG2 deliverable on “Security measures for smart grids” organised on 02.04.2014.<br>Participated in Smart Grid Task Force – Expert Group 2 (managed by EC DG ENER) and provided contributions to the group.  |
| D3   | Algorithms and parameters for secure services (study, Q4)   | “Algorithms, key size and parameters report 2014”<br>Published on 21.11.2014.<br><a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014</a><br>“Study on cryptographic protocols”<br>Published on 21.11.2014.<br><a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols</a>  |
| D4   | Best practice guide for Privacy and Security by Design and Default for the prevention of data leakage and appropriate controls for the access of data (report, Q4)  | “Best practice guide for Privacy and Security by Design and Default”<br>Publication expected by 15.12.2014.<br><a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/</a>   |
| D5   | Auditing framework for trust services: Technical guidelines for independent auditing bodies and supervisory authorities on the implementation of audit schemes for trust service providers in MS. (Report, Q3 2014) | “Auditing framework for trust services”<br>Publication expected by 18.12.2014.<br><a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp-auditing-framework/">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp-auditing-framework/</a>  |
| D6   | Annual Privacy forum 2014 (APF'2014) (Workshop, report, Q2-Q4 2014)   | Forum took place in Athens on 20-21.05.2014.<br>Report: “Privacy Technologies and Policy”<br><a href="http://privacyforum.eu/news/proceedings-apf14-privacy-technologies-and-policy">http://privacyforum.eu/news/proceedings-apf14-privacy-technologies-and-policy</a><br><a href="http://2014.privacyforum.eu/programme">http://2014.privacyforum.eu/programme</a>  |
| <b>WPK1.3 – Supporting the EU in education, research &amp; standardisation</b> |   |  |
| D1   | Inventory of standardisation activities in NIS and Privacy (Workshops, report, Q1-Q4, 2014)   | “Inventory of standardisation activities in NIS and Privacy”<br>Publication expected by 18.12.2014.<br><a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standards-eidas">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standards-eidas</a>   |

|    |   |  |
|----|---|--|
| D2 | Roadmap for the implementation of the "NIS Driving license" | <p>"Cybersecurity competitions — the status in Europe"<br/>Published on 19.11.2014.<br/><a href="https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/cybersecurity-competitions-2014-the-status-in-europe">https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/cybersecurity-competitions-2014-the-status-in-europe</a></p> <p>"Roadmap for NIS education programmes in Europe"<br/>Published on 31.10.2014.<br/><a href="https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe">https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe</a></p> <p>Extra mile:<br/>"Public Private Partnerships in Network and Information Security Education"<br/>Published on 06.10.2014.<br/><a href="https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education">https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education</a></p> |
|----|---|--|

## WS2 – Support Capacity Building

### WPK2.1 – Support Member States' capacity building

|    |  |  |
|----|--|--|
| D1 | Assisting MS in building capabilities on NCSS (workshops, Q1-Q4)   | Workshop on Cyber Security Strategies organised on 27.11.2014.<br><a href="https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop">https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop</a>  |
| D2 | White Paper – How to Evaluate a National Cyber Security Strategy (report, Q3 2014)   | "An evaluation framework for Cyber Security Strategies"<br>Published on 27.11.2014.<br><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies</a> |
| D3 | Good practice guide on training methodologies, etc. for operational teams and communities like CERTs ("Train the trainers handbook") derived from experiences from delivering suitable CERT training (Q4 2014) | "Good Practice Guide on Training Methodologies"<br>Published on 12.11.2014.<br><a href="https://www.enisa.europa.eu/activities/cert/support/exercise/good-practice-guide-on-training-methodologies">https://www.enisa.europa.eu/activities/cert/support/exercise/good-practice-guide-on-training-methodologies</a>   |
| D4 | Regular update of "Baseline capabilities" definition and status and conclusions for new training material (Q4, 2014)   | "Baseline Capabilities" definition and status"<br>Publication expected 18.12.2014.<br><a href="https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/">https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/</a>  |
| D5 | New set of CERT exercise material with at least five new scenarios from the four areas of the "Baseline capabilities", including the topic of processing of actionable operational information (Q4 2014)       | <ol style="list-style-type: none"> <li>1) Developing countermeasures;</li> <li>2) Common framework for artifact analyses activities;</li> <li>3) Advanced artifact handling;</li> <li>4) Processing and storing artifacts;</li> <li>5) Building artifact handling and analyses environment.</li> </ol> Publication expected by 15.12.2014.<br>All available here: <a href="http://www.enisa.europa.eu/activities/cert/training/training-resources">http://www.enisa.europa.eu/activities/cert/training/training-resources</a>            |
| D6 | Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area (Q4 2014)  | "Impact Assessment and Roadmap"<br>Published on 01.12.2014.<br><a href="https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap">https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap</a>   |
| D7 | Assisting MS in building capabilities on national PPPs (workshops, Q1-Q4)  | Panel on PPPs during the National Cyber Security Strategies workshop, 27.11.2014<br><a href="https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop">https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop</a>  |

### WPK2.2 – Support private sector capacity building

|    |   |  |
|----|---|--|
| D1 | Support the Working Groups of the NIS Platform (workshops, contributions, technical support, Q1 – Q4, 2014) | <ol style="list-style-type: none"> <li>1) NIS Platform:               <ul style="list-style-type: none"> <li>- Support DG CNECT - H4 for project Management &amp; coordination of WGs and rapporteurs</li> <li>- Support to DG CNECT - H4 in the organization of the plenary meetings of the 30 April 2014 and the 25th November 2014</li> <li>- User management, mailing lists, online collaboration and content management on the Resilience portal</li> </ul> </li> <li>2) Report "EP3R 2009-2013 future of NIS Private public cooperation"<br/>Publication date 17.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013</a></li> </ol> |
|----|---|--|

|    |  |  |
|----|--|--|
| D2 | White Paper on the Certification of Smart Grids (report, Q3, 2014)   | <p>“Smart grid security certification in Europe”<br/>Publication expected by 18.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification</a></p> <p>Validation workshop for “Smart Grid Components Certification” reports organised on 30.09.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components</a></p>   |
| D3 | White Paper on the Certification of Cyber Security Skills of ICS SCADA experts (report, Q3 2014)                                 | <p>“Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts”<br/>Publication expected by 18.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals</a></p> <p>Validation workshop for the “CERTIFICATION OF CYBER SECURITY SKILLS OF ICS SCADA EXPERTS” report organised on 30.09.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components</a></p> |
| D4 | Harmonised Minimum Security Measures for ISPs (report, Q4 2014)  | <p>“Technical guidelines on security measures for Art.4 and Art.13a”<br/><a href="https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/">https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/</a></p>   |
| D5 | Minimum Security Measures for Cloud Computing (report, Q4, 2014)   | <p>“Cloud Certification Schemes Meta Framework”<br/>Published on 15.11.2014 (in the resilience portal)<br/><a href="https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework">https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework</a></p>   |
| D6 | White Paper - Procurement Guidelines for Secure Cloud Computing Deployment (report, Q4, 2014)                                    | <p>“Security Framework for Governmental Clouds”<br/>Publication expected by 18.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds</a></p>  |
| D7 | Guidelines for the identification of critical services, assets and links in Electronic Communication Networks (report, Q4, 2014) | <p>“Methodologies for the identification of critical information infrastructure assets and services”<br/>Publication expected by 18.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis</a></p>   |
| D8 | Guidelines for Secure Inter-Banking Communications and Transactions (report, Q4, 2014)   | <p>“Network and Information Security in the Finance Sector - Regulatory landscape and Industry priorities”<br/>Publication expected by 17.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector/">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector/</a></p>   |

### WPK2.3 – Raising the level of preparedness of EU citizens

|    |   |  |
|----|---|--|
| D1 | Provide technical guidance and support for European Cyber-Security Month (dissemination material, Q4 2014); | <ol style="list-style-type: none"> <li>1) The launch of the event organised on 01.10.2014. alongside ENISA's high-level event “10 years of securing Europe's cyber security... and beyond!”</li> <li>2) Dissemination materials available at <a href="https://cybersecuritymonth.eu/">https://cybersecuritymonth.eu/</a></li> <li>3) European Cyber Security recommendations for all<br/>Published<br/><a href="http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014">http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014</a></li> <li>4) ESCM 2014 Deployment report<br/>Publication expected by 12.12.2014<br/><a href="https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014">https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014</a></li> </ol> |
|----|---|--|

### WS3 – Support Cooperation

#### WPK3.1 – Crisis cooperation – exercises

|    |   |   |
|----|---|---|
| D1 | Cyber Europe 2014: Exercise Plan and Exercise (exercice, Q4 2014)                         | Exercise organised on 30.10.2014.   |
| D2 | Report on Cyber Crisis Cooperation and Exercise Activities and Findings (report, Q4 2014) | <p>“Report on Cyber Crisis Cooperation and Management”<br/>Published on 06.11.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccs-management/ccs-study">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccs-management/ccs-study</a></p> |
| D3 | EU-US Cybersecurity Exercise Plan   | Was not carried out   |

### WPK3.2 – Implementation of EU legislation

|    |  |  |
|----|--|--|
| D1 | Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents (report, Q2/3 2014) | <p>1) “Annual Incidents report 2013”<br/>Published on 16.09.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013</a></p> <p>2) “Technical Guideline on Incident Reporting V2.1”<br/>Published on 24.10.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting</a></p> <p>3) “Technical Guideline on Security Measures V2.0”<br/>Published on 24.10.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures</a></p> <p>4) Secure ICT Procurement in Electronic Communications<br/>Published on 11.12.2014<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/secure-ict-procurement-in-electronic-communications">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/secure-ict-procurement-in-electronic-communications</a></p> <p>5) Security Guide for ICT Procurement<br/>Published on 11.12.2014<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/security-guide-for-ict-procurement">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/security-guide-for-ict-procurement</a></p> <p>6) “Protection of underground electronic communications infrastructure”<br/>Publication expected by 18.12.2014.<br/><a href="https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure">https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure</a></p> |
| D2 | Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2014)   | Cancelled (Amending WP 2014 )<br>First ENISA workshop with national authorities held in Brussels on the 17.11.2014. Minutes available upon request.  |
| D3 | Support the implementation of the NIS Directive (workshops, Q2-Q4)   | Cancelled (Amending WP 2014)   |

### WPK3.3 – Regular cooperation among NIS communities

|    |  |  |
|----|--|--|
| D1 | 9th ENISA CERT workshop to prepare a roadmap for future work of ENISA in the area of CERT training and CERT cooperation with LEA (in cooperation with EC3)(Q4) | ENISA 9th annual workshop ‘CERTs in Europe’ – Part I organised on 27-28.05.2014.<br>The ENISA 9th annual workshop ‘CERTs in Europe’ - Part II organised on 13-14.10.2014.  |
| D2 | Good practice guide and / or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs (Q4 2014)    | “Best practice guide on exchange processing of actionable information – exercise material”<br>Publication expected by 18.12.2014<br><a href="https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf">https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf</a>                      |
| D3 | Draft report “Stocktaking on channels and formats for exchange of operational information”   | “Stocktaking of standards formats used in exchange of processing actionable information”<br>Publication expected by 18.12.2014<br><a href="https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf">https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf</a>                        |
| D4 | Draft report “Scalable and accepted methods for trustbuilding within and among communities”  | “Scalable and Accepted Methods for Trust Building in Operational Communities”<br>Published on 27.11.2014.<br><a href="https://www.enisa.europa.eu/activities/cert/support/information-sharing/scalable-and-accepted-methods-for-trust-building">https://www.enisa.europa.eu/activities/cert/support/information-sharing/scalable-and-accepted-methods-for-trust-building</a>             |
| D5 | Good practice material for first responders in cooperation with the EC3 (Q4)   | “Good practice material for first responders”<br>Publication expected by end of December 2014<br><a href="https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders/">https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders/</a> |

#### Flash notes:

Flash Note: Heartbleed - A wake-up call  
Published on 14.04.2014.

<https://www.enisa.europa.eu/publications/flash-notes/flash-note-heartbleed-a-wake-up-call>

Flash Note: Large scale UDP attacks - the 2014 trend and how to face it  
Published on 24.02.2014.

<https://www.enisa.europa.eu/publications/flash-notes/large-scale-udp-attacks-the-2014-trend-and-how-to-face-it>

Flash note: Risks of using discontinued software  
Published on 29.01.2014.

<https://www.enisa.europa.eu/publications/flash-notes/flash-note-risks-of-using-discontinued-software>