FOLLOW-UP EP LIBE RESOLUTIONS: ROADMAP & ACTION PLAN

PAR.	LIBE RESOLUTION
101	Calls on the competent services of the Secretariat of the European Parliament, under the responsibility of the President of Parliament, to carry out, by June 2015 at the latest with an intermediate report by December 2014 at the latest, a thorough review and assessment of Parliament's IT security dependability, focused on: budgetary means, staff resources, technical capabilities, internal organisation and all relevant elements, in order to achieve a high level of security for Parliament's IT systems; believes that such an assessment should at the least provide information, analysis and recommendations on:

LIBE REQUESTS TO EU ICT SECURITY - EUROPEAN PARLIAMENT	ITEC ROADMAP & ACTION PLAN
- The need for regular, rigorous and independent security audits and penetration tests, with the selection of outside security experts ensuring transparency and guarantees of their credentials vis-à-vis third countries or any types of vested interest;	The European Parliament administration is aware that 100% security can never be achieved and that both procedures and technologies in use must be continuously reviewed. This is why together with a prompt implementation of the security patches available the EP is performing regular assessments on the security aspects of the systems. However, ITEC will organise an external independent audit on IT security system (see also EP Resolution on 2012 discharge P7_TA-PROV(2014)0428, paragraph 90)
- the inclusion in tender procedures for new IT systems of best-practice specific IT security/privacy requirements, including the possibility of a requirement for open source software as a condition of purchase or a requirement that trusted European companies should take part in the tender when sensitive, security-related areas are concerned;	Call for tenders specifications must strictly follow the Public Procurement Regulation and at moment respect the principle of equal treatment hence no such limitations can be built in the specifications
- the list of companies under contract with Parliament in the IT and telecom fields, taking into account any information that has come to light about their cooperation with intelligence Agencies (such as revelations about NSA contracts with a company such as RSA, whose products Parliament is using to supposedly protect remote access to their data by its Members and staff), including the feasibility of providing the same services by other, preferably European, companies;	Call for tenders specifications must strictly follow the Public Procurement Regulation, at moment respect the principle of equal treatment and not impose artificial limitations to the competition hence no such limitations can be built in the specifications unless the Public Procurement Regulation is amended or a mechanism of blacklisted companies is established by law.
- the reliability and resilience of the software, and especially off-the-shelf commercial software, used by the EU institutions in their IT systems with regard to penetrations and intrusions by EU or third-country law enforcement and intelligence authorities, taking also	The ICTSECU service, inside DG ITEC, is actively collaborating with CERT-EU on these matters. CERT-EU has organised several technological workshops where major vendors reliability were assessed. It is also exchanging on a daily basis information about

into account relevant international standards, best-practice security risk management principles, and adherence to EU Network Information Security standards on security breaches;	vulnerabilities and Indication of Compromise (IOC) The following strategy is proposed: - Organise bilateral meetings with all ICT system owners and define the scope of the assessment. - Configure the scan engines, perform an initial assessment, fine tune the configuration, and start Internal vulnerability assessment: The ICTSECU service is operating a vulnerability assessment platform. Currently, the scope of the assessment is limited and not systematic. It is proposed to make this assessment mandatory for all systems operated at the EP by verifying reports on a weekly basis.
- the use of more open-source systems;	The internal IT product selection stipulates that in the context of a new product acquisition, if it is specified that an open source system is providing the same level of services (including requirement coverage, support and sustainability) than a proprietary one, the open source solution is to be chosen.
- steps and measures to take in order to address the increased use of mobile tools (e.g. smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;	It is important to remind that the European Parliament administration has already taken care of the mobility aspects for laptops by providing a Multi-boot solution where the standard configuration is encrypted. This solution, when running outside the EP premises, is able to connect to the EP network via secure connections. Progress: • October 2014: more than 1000 Ipads have been deployed for EP Staff, with a security policy enforced by an MDM (Mobile Device Management) solution (Movep project). Security policy and awareness have been developed and communicated to users. • Additional devices are being deployed for MEPs, based on the same configuration • Then, all personal mobile devices used to access EP information or systems will be secured. • Finally, all corporate smartphones will be included in the same management system.
- the security of the communications between the different workplaces of the Parliament and of the IT systems used in Parliament;	A risk assessment has to be done, as the current provider has claimed that its communication network was not accessed by the NSA. Deployment of encryption solutions would require a careful analysis to prevent degradation of service of the high capacity links between workplaces of the Parliament.

- the use and location of servers and IT centres for Parliament's IT systems and the implications for the security and integrity of the systems.	The central IT server infrastructures are located in two main datacentres and additional smaller rooms. The two main datacentres are located outside EP premises. They are linked to contract with operators providing rooms, cooling, power and physical security access control. The accesses to the two datacentres are permanently controlled. All accesses are registered and need EP authorisations. Card readers are used to allow access to the rooms. Connexion between Datacentres and EP premises are realised on a private network as for the different workplaces of the Parliament. Additional smaller rooms are located in EP premises and have access control card readers linked to EP security services in place.
- the implementation in reality of the existing rules on security breaches and prompt notification of the competent authorities by the providers of publicly available telecommunication networks;	The Parliament already receives security information from normal channels and should improve the process to anticipate as much as possible the notifications,
- the use of cloud computing and storage services by Parliament, including the nature of the data stored in the cloud, how the content and access to it is protected and where the cloud-servers are located, clarifying the applicable data protection and intelligence legal framework, as well as assessing the possibilities of solely using cloud servers that are based on EU territory;	An inter-institutional initiative has been started on Cloud solutions. The Parliament is actively participating to it: concrete results should be submitted during 2015.
- a plan allowing for the use of more cryptographic technologies, in particular end-to-end authenticated encryption for all IT and communications services such as cloud computing, email, instant messaging and telephony;	October 2014 - ICTSECU service has performed a study on email encryption, for occasional use. A suitable product has been identified and is available. The packaging and documentation for the use of this product has been finalised; this would allow the fast deployment of this solution in case of needs. Specific needs (DG EXPO, DG PERS) expressed within the institution have already been addressed and impact study has to be started to evaluate how the applied solution can be generalised.
- the use of electronic signatures in email;	October 2014 - A pilot project of email signature and encryption, using keys stored on the service card has been run successfully. A strategic decision has to be taken to deploy it for all EP users, or the re-assess the technology in a new pilot project study has to be started to evaluate how the applied solution can be generalised.

- a plan for using a default encryption standard, such as the GNU Privacy Guard, for emails that would at the same time allow for the use of digital signatures;	The PGP standards has been selected (instead of GPG) and implemented. Deployment can start in case of need and as soon as licenses are provided. The SMIME standard has been also selected and implemented for specific needs. Choice will depend on needs and involved
- the possibility of setting up a secure instant messaging service within Parliament allowing secure communication, with the server only seeing encrypted content;	Status: not started. Encryption aspects have to be carefully analysed for avoiding compatibility problems that could generate service disruption,