EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung des IKT-Schlüsselprojektes Interception System Schweiz 2

Eidgenössisches Justiz- und Polizeidepartement

EFK-14393 / inkl. Stellungnahmen / 29. Juli 2014

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch/
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.14393.485.00148.05
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	Fachbereich 7: IKT-Schlüsselprojekt-Prüfungen E-Mail: martin.schwaar@efk.admin.ch Tel. 058 465 33 23
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung **Résumé** **Riassunto** **Summary**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») Italiano (« L'essenziale in breve ») English (« Key facts »)

Das Wesentliche in Kürze

Gestützt auf die Weisungen des Bundesrates für IKT-Schlüsselprojekte prüfte die Eidgenössische Finanzkontrolle EFK im Zeitraum von April bis Juni 2014 beim Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) das Projekt Interception System Schweiz (ISS 2). Ziel der Prüfung war es, den Projektstand und die Risiken hinsichtlich der Zielerreichung zu beurteilen.

Mit dem heute eingesetzten System zur Fernmeldeüberwachung kann der Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF) seinem gesetzlichen Auftrag nicht mehr gerecht werden. Zur Aufklärung von schweren Straftaten oder für Notsuchen führt dieser Dienst auf Anordnung der Staatsanwaltschaften und mit Genehmigung der zuständigen Gerichte Fernmeldeüberwachungen durch. Zu diesem Zweck betreibt das ISC-EJPD das „Lawful Interception System» (LIS), welches die Daten der Fernmeldeanbieter entgegen nimmt und den Strafverfolgungsbehörden zur Verfügung stellt. LIS ist “end of life“ und muss abgelöst werden. Zu diesem Zweck wurde im Jahr 2008 das Projekt Interception System Schweiz (ISS 1) initialisiert.

Im Rahmen eines auf dem Bundesgesetz über das öffentliche Beschaffungswesen (BöB) Art. 3 begründeten Einladungsverfahrens wurde der Lieferant für ISS 1 gewählt. Das Projekt wurde im Jahr 2013 aus verschiedenen Gründen abgebrochen und unter dem Namen ISS 2 mit einer Schwesterfirma eines Alternativ-Anbieter aus demselben Einladungsverfahren neu aufgesetzt. Der vorliegende Bericht bezieht sich auf das laufende Projekt ISS 2.

Trotz Handlungsbedarf ist das Projekt ISS 2 insgesamt auf Kurs. Die Termin- und Finanzrisiken bezüglich des für März 2015 geplanten Produktivstarts werden angemessen kontrolliert. Das Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) ist noch nicht genehmigt. Sollten hier noch Auflagen erfolgen und Anpassungen notwendig werden, könnten sich diese negativ auf den Projektverlauf auswirken.

Die Projektorganisation ist zweckmässig. Der Projektumfang ist klar definiert und die Projektorganisation ist schlank aufgebaut. Die wichtigsten Anspruchsträger sind über den Projektausschuss eingebunden, welcher durch den Generalsekretär des EJPD als Projektauftraggeber geführt wird.

Die Lösungsarchitektur erfordert begleitende Massnahmen bei der Umsetzung und für den Betrieb. Entsprechend dem Projektauftrag wurde ein Basis-System definiert, welches nicht redundant ausgelegt ist und die minimalen Anforderungen zur Sicherstellung des heutigen gesetzlichen Auftrages erfüllt. Die Datenmengen, welche das System und die ein- und ausliefernden Netzwerke zukünftig verarbeiten müssen, sind nur schwer abschätzbar. Dies insbesondere, weil sich die Telefonie weg von der herkömmlichen Technologie hin zu Voice over IP und weiteren Internetdiensten mit zunehmendem Anteil an multimedialen Inhalten bewegt. Hinzu kommt, dass sich die Entwicklung der Anzahl Überwachungen nur schwer abschätzen lässt. Eine vorsorgliche grosszügige Dimensionierung von ISS 2 wäre ein unwirtschaftliches Vorgehen, weshalb das Projekt einen anderen Ansatz verfolgt. Um allfällige Dateneinleitungs-Spitzen zu kompensieren oder negative Auswirkungen der fehlenden Redundanz zu verringern, soll dem Basis-System ein neu zu entwickelndes Buffersystem vorgelagert werden. Das entsprechende Konzept ist jedoch noch nicht

fertig gestellt und es ist auch noch nicht entschieden, ob es intern entwickelt oder extern ausgeschrieben werden soll. Aus Sicht EFK wird dem Buffersystem im Projekt nicht die notwendige Priorität eingeräumt.

Die beschriebenen Unsicherheiten bezüglich Dimensionierung betreffen gleichermassen auch das Buffersystem und können durch dieses nur teilweise entschärft werden. Ein Ausbau der Kapazitäten tangiert immer sämtliche Komponenten in der Verarbeitungskette. Die EFK empfiehlt dem EJPD, die Kapazitätsberechnungen ab Produktivstart anhand der effektiv eingeleiteten Datenmenge regelmässig zu überprüfen und bereits jetzt die Pläne für einen allfällig notwendigen Systemausbau zu erstellen.

Angesichts der fehlenden Redundanz des Basis-Systems kommt dem Continuity Management eine zentrale Rolle zu. Im Bereich Business Continuity Management (BCM) ist der Dienst ÜPF bereits am Erarbeiten entsprechender Konzepte. Das IT Service Continuity Management (ITSCM) sieht heute vor, dass das Integrations-System im Katastrophenfall zum Produktiv-System umgebaut wird, konkretisiert ist dies jedoch nicht. Aus Sicht der EFK müssen bereits vor dem Produktivstart detaillierte Notfallpläne mit Drehbüchern vorliegen.

Sicherheitsanforderungen sind noch nicht alle konzipiert. Der Schutzbedarf wurde ermittelt, die Anforderungen an die Sicherheit sind bekannt. Das ISDS-Konzept ist jedoch in Verzug, es sollte mit hoher Priorität fertig gestellt werden. Das Berechtigungskonzept ist noch vor Inbetriebnahme von ISS 2 umzusetzen.

L'essentiel en bref

Conformément aux directives du Conseil fédéral concernant les projets informatiques clés, le Contrôle fédéral des finances (CDF) a effectué durant la période allant d'avril à juin 2014 l'audit du projet Interception System Schweiz (ISS 2) auprès du Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP). Le CDF était chargé d'examiner l'état d'avancement du projet et les risques susceptibles de compromettre l'atteinte des objectifs.

Le système de surveillance des télécommunications utilisé actuellement ne permet plus au Service de surveillance de la correspondance par poste et télécommunication (service SCPT) d'exécuter son mandat légal. Sur ordre des ministères publics et après autorisation des tribunaux compétents, ce service accomplit des tâches de surveillance des télécommunications visant à élucider des infractions graves ou à retrouver des personnes disparues. Pour ce faire, le CSI-DFJP exploite le système LIS (*Lawful Interception System*), qui lui permet de récupérer des données auprès des fournisseurs de services de télécommunication et de mettre ces informations à la disposition des autorités de poursuite pénale. Le système LIS étant arrivé au terme de son cycle de vie, son remplacement est inévitable. Le projet Interception System Schweiz (ISS 1) avait été lancé à cet effet en 2008.

Dans le cadre de l'art. 3 de la loi fédérale sur les marchés publics (LMP), une procédure invitant à soumissionner avait permis de sélectionner un fournisseur pour ISS 1. En 2013, le projet avait été interrompu pour des raisons diverses. Rebaptisé ISS 2, le projet a pris un nouveau départ avec une société sœur d'un autre fabricant issu de la même procédure. Le présent rapport concerne le projet actuel ISS 2.

Malgré la nécessité de certaines mesures, le projet ISS 2 est sur la bonne voie. Les risques liés aux délais et aux coûts sont correctement examinés en vue du lancement prévu pour mars 2015. Le concept de sûreté de l'information et de protection des données (concept SIPD) n'a pas encore été validé. Le déroulement du projet pâtirait de l'ajout de nouvelles exigences et des adaptations qui s'avéreraient nécessaires.

L'organisation du projet répond aux attentes. L'étendue du projet est clairement définie et l'organisation adéquate. Les principales parties prenantes ont été associées aux travaux par l'intermédiaire du comité de projet, dirigé par le secrétaire général du DFJP en tant que mandant.

L'architecture de solution exige des mesures d'accompagnement en vue de la mise en œuvre et de l'exploitation. Comme le prévoyait le mandat de projet, le système de base défini n'a pas été conçu de manière redondante. Il satisfait aux exigences minimales qui permettent de remplir l'actuel mandat légal. La quantité de données que le système et les réseaux traitant les informations entrantes et sortantes devront gérer est difficile à déterminer. En effet, la téléphonie traditionnelle laisse peu à peu place à celle passant par Internet (*Voice over IP*) ainsi qu'à d'autres services fournis sur le Web, créant ainsi de plus en plus de contenus multimédias. L'évolution du nombre de surveillances est elle aussi difficile à prévoir. Il ne serait pas rentable de donner dès à présent une ampleur trop importante à l'ISS 2. C'est pourquoi le projet suit une approche différente. Pour compenser les éventuels pics au niveau de l'entrée des données et réduire les conséquences négatives de l'absence de redondance, un système tampon, qui doit encore être élaboré, devra

compléter le système de base. Cependant, le concept correspondant n'est pas encore achevé. Il n'a en outre pas encore été décidé si le système sera développé au sein de l'administration fédérale ou mis au concours. Selon le CDF, le projet ne tient pas suffisamment compte de la priorité du système tampon.

Les incertitudes mentionnées quant à l'ampleur du système de base regardent également le système tampon, qui est seulement à même de les lever partiellement. Le développement des capacités concerne toujours la totalité des composants d'une chaîne de transformation. C'est pourquoi le CDF recommande au DFJP de contrôler régulièrement le calcul des capacités dès le lancement, et ce, au moyen des quantités effectives de données entrantes, et de préparer d'ores et déjà un éventuel développement du système.

En raison de l'absence de redondance dans le système de base, la gestion de la continuité joue un rôle central. Le service SCPT élabore actuellement les projets nécessaires dans le domaine de la gestion de la continuité des affaires (Business Continuity Management, BCM). La gestion de la continuité des services informatiques prévoit aujourd'hui une transformation du système d'intégration en système productif en cas de catastrophe, mais cela n'a pas encore été concrétisé. Selon le CDF, des plans d'urgence détaillés ainsi que divers scénarios devront être disponibles avant le lancement.

Certaines exigences en matière de sécurité restent à concevoir. Les besoins de protection sont établis et les exigences en matière de sécurité définies. Cependant, le concept SIPD a pris du retard. Par conséquent, son élaboration doit bénéficier d'une priorité majeure. En outre, le concept d'autorisations doit être mis en œuvre avant le lancement de l'ISS 2.

Texte original en allemand

L'essenziale in breve

Conformemente alle istruzioni del Consiglio federale concernenti i progetti chiave TIC, tra aprile e giugno del 2014 il Controllo federale delle finanze (CDF) ha esaminato presso il centro servizi informatici del Dipartimento federale di giustizia e polizia (ISC-DFGP) il progetto «Interception System Schweiz» (ISS 2) («Sistema di intercettazione per la Svizzera»). La verifica mirava a valutare lo stato del progetto e i rischi in relazione al raggiungimento degli obiettivi.

Con il sistema attualmente impiegato per la sorveglianza in remoto il Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (SCPT) non adempie più il suo mandato legale. Questo servizio effettua la sorveglianza in remoto su richiesta dei ministeri pubblici e con l'autorizzazione dei tribunali competenti per chiarire gravi reati o per effettuare ricerche urgenti. A tal fine l'ISC-DFGP gestisce il «Lawful Interception System» (LIS) («Sistema di intercettazione legale») che riceve i dati dei fornitori di servizi di telecomunicazioni e li mette a disposizione delle autorità di perseguimento penale. Il LIS è al termine del suo ciclo di vita e deve essere sostituito. A tale scopo nel 2008 è stato avviato il progetto «Interception System Schweiz» (ISS 1).

Nel quadro di una procedura mediante invito basata sull'articolo 3 della legge federale sugli acquisti pubblici (LAPub) è stato scelto un fornitore per l'ISS 1. Nel 2013 il progetto è stato interrotto per diversi motivi ed è stato riformulato con il nome ISS 2 con una società affiliata di un altro offerente che aveva partecipato alla stessa procedura mediante invito. Il presente rapporto si riferisce all'attuale progetto ISS 2.

Nel complesso, nonostante la necessità d'intervento il progetto ISS 2 avanza. I rischi finanziari e quelli legati alle scadenze, relativi all'inizio dell'operatività programmato per il mese di marzo del 2015, vengono adeguatamente controllati. Il progetto sulla sicurezza dell'informazione e della protezione dei dati (progetto SIPD) non è ancora stato approvato. Se dovessero essere create altre condizioni e fossero necessari adeguamenti, questi si potrebbero ripercuotere negativamente sullo svolgimento del progetto.

L'organizzazione del progetto è adeguata. L'entità del progetto è definita chiaramente e la sua organizzazione è snella. I principali stakeholder sono coinvolti da un comitato del progetto diretto dal segretario generale del DFGP in qualità di committente.

L'architettura della soluzione richiede misure accompagnatorie per l'attuazione e l'esercizio. Conformemente al mandato del progetto è stato definito un sistema di base che non è concepito in maniera ridondante e soddisfa i requisiti minimi per garantire l'attuale mandato legale. È difficile stimare le quantità di dati che in futuro dovranno essere elaborate dal sistema e dalle reti che li trasmettono, in particolare perché la telefonia si sta spostando dalla tecnologia tradizionale verso il voice over IP (VOIP) e altri servizi Internet prevedono un crescente numero di contenuti multimediali. Inoltre, è difficile stimare l'evoluzione del numero di intercettazioni. Un sovradimensionamento a titolo preventivo dell'ISS2 sarebbe un modo di procedere antieconomico, perché il progetto segue un altro approccio. Per compensare eventuali picchi nell'inserimento dei dati o ridurre le ripercussioni negative della ridondanza mancante, il sistema di base deve prevedere un sistema buffer che deve essere ancora sviluppato. Tuttavia, il relativo progetto non è

ancora stato completato e non è ancora stato deciso se sarà sviluppato internamente o assegnato all'esterno. Secondo il CDF nel progetto non viene accordata la priorità necessaria al sistema buffer.

Le incertezze descritte in merito alle dimensioni riguardano in egual misura anche il sistema buffer che le può attenuare solo in parte. Un ampliamento delle capacità si ripercuote sempre su tutti i componenti della catena dell'elaborazione. Il CDF raccomanda al DFGP di verificare regolarmente i calcoli delle capacità dall'inizio dell'operatività in base alla quantità di dati effettivamente inseriti e di predisporre già ora i piani per un ampliamento del sistema che si rendesse eventualmente necessario.

Alla luce della ridondanza mancante del sistema di base il Continuity Management riveste un ruolo di primaria importanza. Nell'ambito del Business Continuity Management (BCM) l'SCPT sta già predisponendo i relativi progetti. L'IT Service Continuity Management (ITSCM) prevede attualmente che in caso di catastrofi il sistema di integrazione al sistema produttivo sia riformulato, ma ciò non è stato ancora realizzato. Secondo il CDF già prima dell'avvio dell'operatività devono essere disponibili piani di emergenza dettagliati con le istruzioni.

I requisiti di sicurezza non sono ancora stati completamente concepiti. La necessità di protezione è stata comunicata, mentre le esigenze di sicurezza sono note. Dato che è in ritardo, il progetto ISDS dovrebbe essere concluso con la massima priorità. Il piano delle autorizzazioni deve essere attuato prima dell'attivazione dell'ISS 2.

Testo originale in tedesco

Key facts

In accordance with the Federal Council's directives for key ICT projects, from April to June 2014, the Swiss Federal Audit Office (SFAO) audited the Interception System Switzerland (ISS 2) project at the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP). The audit's aim was to assess the project status and risks with regard to the achievement of targets.

The Post and Telecommunications Surveillance Service (PTSS) can no longer fulfil its legal mandate with the current system used for telephone tapping. This Service carries out telephone tapping at the request of the public prosecutors and with the approval of the courts responsible for the investigation of serious offences and for emergency searches. To this end the ISC-FDJP operates the Lawful Interception System (LIS) which receives the data from the telecom operators and makes this available to the criminal prosecution authorities. LIS is at the end of its operational life and must be replaced. For this purpose, the Interception System Switzerland (ISS 1) project was initialised in 2008.

The ISS 1 supplier was selected within the scope of a tender invitation procedure based on Article 3 of the Federal Act on Public Procurement (PPA). In 2013, the project was abandoned for various reasons and relaunched under the name ISS 2 with a sister company of an alternative provider from the same tender procedure. This report refers to the current ISS 2 project.

In spite of the need for action, overall the ISS 2 project is on course. The schedule and financial risks for the operational start planned for March 2015 are being kept appropriately in check. The information security and data protection concept (ISDP concept) has not yet been approved. Should this result in requirements and adjustments, it could have a negative impact on the progression of the project.

Project organisation is expedient. The scope of the project has been clearly defined and the structure of the project organisation is lean. The most important stakeholders are involved via the project committee which is managed by the Secretary General of the FDJP as the project manager.

The solution architecture requires accompanying measures for implementation and operation. In line with the project brief, a basic system was defined which is not redundant in design and fulfils the minimum requirements on guaranteeing the current statutory mandate. The data amounts which the system and the receipt and delivery networks will have to process in the future are difficult to predict. This is in particular because telephony is moving away from conventional technology to voice-over IP and other Internet services with an increasing amount of multimedia content. Added to this is the fact that the development of the amount of monitoring is difficult to predict. Precautionary, generous dimensioning of ISS 2 would be an uneconomic course of action which is why the project is pursuing a different approach. So as to compensate for any data entry peaks and to reduce the negative impact of the lack of redundancy, the basic system should be preceded by a buffer system which has yet to be developed. However, the corresponding concept has not yet been finalised and it has not yet been decided whether or not it will be developed internally or put out to tender. From the perspective of the SFAO, the required priority has not been accorded to the buffer system in the project.

The uncertainties described above relating to dimensioning apply equally to the buffer system and they may be only partially alleviated by the buffer system. Upgrading the capacity always affects all components in the processing chain. The SFAO recommends that the FDJP regularly examine the capacity calculations from the time production starts on the basis of the amount of data effectively entered and to draw up now an expansion of the system that may prove necessary.

In view of the lack of redundancy of the basic system, continuity management plays a central role. In the area of business continuity management, the PTSS is already drawing up corresponding concepts. The IT Service Continuity Management is today making provision for the integration system to be converted to a productive system in the event of a disaster. However, this has not been fleshed out. From the perspective of the SFAO, detailed emergency plans with scenarios must be available already before the operational start.

Security requirements have not yet all been drawn up. Protection requirements have been determined and security requirements are known. However, the ISDP concept is behind schedule; its completion should be given high priority. The authorisation concept must be implemented before putting ISS 2 into operation.

Original text in German

Generelle Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements zur Prüfung:

Die Überprüfung des Projektes ISS durch die EFK ergab wertvolle Hinweise, welche für den weiteren erfolgreichen Projektverlauf sehr hilfreich sein werden. Das EJPD wird die durch die EFK ausgesprochenen Empfehlungen übernehmen und umsetzen. Aufgrund der dringlichen Einführung des Alternativsystems kann allerdings nicht garantiert werden, dass bereits bei der Inbetriebnahme des Systems alle durch die EFK formulierten Empfehlungen umgesetzt sein werden. Dies zumal es sich beim aktuell zu beschaffenden System um ein sogenanntes Basissystem handelt, welches entsprechend den diesbezüglichen Vorgaben nicht allen Anforderungen genügt. Um dieses Manko beheben zu können, bedarf es weiterer Systemausbauten und Leistungssteigerungen, welche zum Teil erst mit der Realisierung der in Planung befindlichen Folgeprojekte umgesetzt werden können (Programm FMÜ). Zur Finanzierung dieses Programms wird derzeit eine Botschaft erstellt.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Gestützt auf die Weisungen des Bundesrates[1] prüft die Eidg. Finanzkontrolle (EFK) IKT-Schlüsselprojekte des Bundes. Ein IKT-Schlüsselprojekt ist ein Projekt oder Programm, das wegen seines Ressourcenbedarfs, seiner Komplexität, seiner Auswirkungen oder Risiken einer verstärkten übergeordneten Führung, Steuerung, Koordination und Kontrolle bedarf.

Die Bestimmung der IKT-Schlüsselprojekte ist Gegenstand eines jährlichen Beschlusses des Bundesrats und wird nicht von der EFK geprüft. Die EFK führt die Prüfungen im Rahmen des Finanzkontrollgesetzes durch. Die Verantwortung für die Steuerung, Führung und Kontrolle der IKT-Schlüsselprojekte bleibt unverändert bei der entsprechenden Verwaltungseinheit (Projektverantwortliche und übergeordnete Linie).

Das Projekt Interception System Schweiz 2 (ISS 2) wurde im Mai 2014 vom Bundesrat als IKT-Schlüsselprojekt definiert.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung ist es, den Projektstatus und die Risiken hinsichtlich der Zielerreichung, sowie des künftigen Betriebs und der künftigen Pflege von ISS 2 zu beurteilen. Dazu sollen folgende Fragestellungen dienen:

- Unterstützen Projektauftrag und Projektvorgehen die übergeordneten Ziele, im Speziellen den gesetzlichen Auftrag des ISC-EJPD?
- Entspricht die Architektur der Lösung dem Stand der Technik, sowie internen und externen Richtlinien?
- Erlauben die Rahmenbedingungen eine erfolgreiche Umsetzung des Projekts?
- Ist das Projektmanagement (Planung, Organisation, Controlling, Steuerung) dazu geeignet, die gesetzten Ziele erreichen zu können?
- Werden die Ressourcen (Finanzen, Personal) zielführend eingesetzt?
- Sind die Risiken bezüglich Einhaltung von Terminen und Budget unter Kontrolle?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Martin Schwaar (Leitung) und Frank Ihle im Zeitraum von Mai bis Juni 2014 durchgeführt. Sie basiert auf Interviews mit Schlüsselpersonen auf allen Stufen der Projektorganisation, ergänzt durch eine kritische Beurteilung der Projektdokumentation und ausgewählten Lieferergebnissen.

Die Prüfung beschränkte sich auf das laufende Projekt ISS 2. Wo nötig wurden Informationen aus dem abgebrochenen und zwischenzeitlich abgeschlossenen Vorgängerprojekt ISS 1 berücksichtigt.

[1] Weisungen des Bundesrates für IKT-Schlüsselprojekte vom 27. März 2013

Die Prüfungsbeurteilung basiert auf den aktuellen Entwürfen der Konzepte, insbesondere des ISDS-Konzepts (Version 0.8 vom 14.4.2014). Allfällige Anpassungen im Zusammenhang mit der Genehmigung des ISDS-Konzeptes könnten Einfluss auf den Projektverlauf haben.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von allen Beteiligten in offener und konstruktiver Weise erteilt. Die EFK hatte Zugriff auf sämtliche relevanten Projektunterlagen.

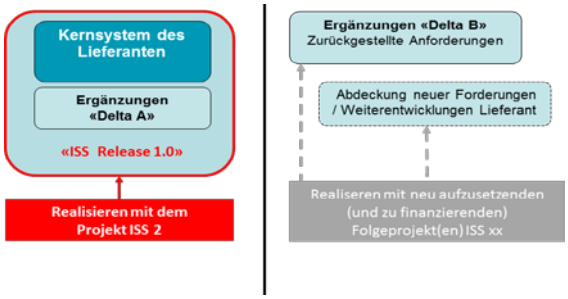
2 Projekt ISS 2: Ablösung des Vorgängersystems LIS

Der Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) führt zur Klärung schwerer Straftaten Post- und Fernmeldeüberwachungen sowie Notsuchen durch, dies auf Anordnung der Staatsanwaltschaften und mit Genehmigung der zuständigen Gerichte. Die angeforderten Daten holt der Dienst bei den betroffenen Fernmeldedienstanbieter (FDA) ein. Zur Entgegennahme und zur Bereitstellung der eingeforderten Daten zu Handen der Strafbehörden betreibt der Dienst ÜPF ein Verarbeitungssystem. Das bisherige System hat das Ende seines Lebenszyklus erreicht und eine Ersatzbeschaffung ist daher notwendig. Das diesbezügliche Beschaffungsprojekt wurde bis zur Einberufung des ad hoc Projektausschusses, unter der Leitung des Dienstes ÜPF und in enger Zusammenarbeit mit den Vertretungen der Strafverfolgungsbehörden, den FDA und des ISC-EJPD im Rahmen des Projekts Interception System Schweiz (ISS) geführt.

Das ursprüngliche Beschaffungsprojekt hatte sich aufgrund technischer Komplikationen und Lieferschwierigkeiten mehrfach verzögert. Nach umfangreichen Abklärungen im Auftrag des gemeinsamen Lenkungsgremiums Fernmeldeüberwachung (LG FMÜ) von Bund, Kantonen, Strafverfolgungsbehörden und Fernmeldedienstanbieterinnen (FDA) kam das LG FMÜ in der Sitzung vom 20. September 2013 zum Schluss, dass eine Fortsetzung des Projekts ISS mit der bisherigen Herstellerin nicht erfolgversprechend ist. Die Departementsleitung hat daraufhin auf Empfehlung des LG FMÜ beschlossen, die Zusammenarbeit mit der Herstellerin des ISS zu beenden und unter dem Namen ISS 2 mit einer Schwesterfirma eines Alternativ-Anbieters aus demselben Einladungsverfahren neu aufzusetzen. Aktuell befindet sich das Projekt in der Phase Realisierung.

Die Gesamtziele des Projekts sind durch die vorstehend beschriebene Ausgangslage bestimmt. Das Projekt ISS 2 ist erfolgreich abgeschlossen, wenn:

- der Gesamtprozess des Schaltens einer Massnahme, der Anlieferung, Verarbeitung und Ausleitung der Daten, sowie der Durchführung der Überwachung bezüglich den organisatorischen Prozessen, dem technischen Durchlauf und der Funktionalität gemäss den Spezifikationen („Usability“ und „Warranty“) produktiv eingesetzt und von allen Stakeholders beherrscht wird.
- die Nachbearbeitung der Daten und Lieferung zur Nutzung durch die Strafbehörden organisatorisch, administrativ und technisch operationell ist.
- die organisatorische und administrative Führung des FMÜ Prozesses von der Anordnung der Bearbeitung, der Steuerung der Überwachung bis zur Aufhebung von Massnahmen im neuen Umfeld gemäss den gesetzlichen Vorgaben operationell sind.
- Mit dem Projekt werden lediglich die minimalen Anforderungen zur Sicherstellung des heutigen gesetzlichen Auftrages umgesetzt (Delta A). Sämtliche darüber hinausgehenden Anforderungen werden in das sogenannte Delta B verschoben, welches zusammen mit Folgeprojekten und der Weiterentwicklung gesondert in Angriff genommen werden muss.



Bereits heute ist klar, dass nach Abschluss des Projektes ISS 2 weitere Ersatzinvestitionen, Anpassungen infolge der Gesetzesrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) beim Dienst ÜPF sowie Anpassungen bei den polizeilichen Informationssystemen der fedpol notwendig werden. Gemäss einem dem Bundesrat unterbreiteten Aussprachepapier geht das EJPD davon aus, dass diese Arbeiten bis ins Jahr 2021 Investition in der Höhe von rund 91 Millionen Franken auslösen werden.

Beurteilung

Mit dem Aussprachepapier schafft das EJPD die notwendige Transparenz über den Investitionsbedarf der nächsten Jahre im Bereich der Überwachung des Post- und Fernmeldeverkehrs. Aus Sicht der EFK kann damit ein allfälliger Vorwurf bezüglich etappenweisen Vorgehens ausgeräumt werden.

3 Projektmanagement

3.1 Die Projektorganisation entspricht der Komplexität der Vorhabens und die Managementattention ist vorhanden

Die Projektorganisation orientiert sich an der Methodik HERMES 5 und ist dem Projektscope (Beschaffung und Installation des Basissystems) entsprechend aufgebaut. Projektauftraggeber (PAG) und Vorsitzender des Projektausschusses (PA) ist der Generalsekretär EJPD. Der PA setzt sich aus dem Projektleiter, dem Kommandanten der Kantonspolizei Bern (KAPO BE) als Vertreter der Konferenz der kantonalen Polizeikommandanten (KKPKS), dem Leiter der Bundesanwaltschaft, dem Stab der Departementsleitung EJPD sowie einem externen Berater zusammen. Im Projektmanagementplan (PM-Plan) sind die Rollen des Projektauftraggebers und der PA-Mitglieder beschrieben und die Aufgaben, Kompetenzen und Verantwortungen (AKV) definiert.

Zusätzlich zum PAG wurden der Kommandant der KAPO BE als Vertreter der KKPKS und der Leiter der Bundesanwaltschaft als Teil-Projektauftraggeber bestimmt. Sie sind für die Durchsetzung der Projektanweisungen und Ressourcenbereitstellungen (Finanzen und Personal) in ihren Bereichen verantwortlich und stellen damit den «verlängerten Arm» des PAG dar. Infolge des grossen Erfolgsdrucks für ISS 2 wurde das Projekt als Standardtraktandum in der Geschäftsleitung des ISC-EJPD definiert und wird dort wöchentlich behandelt.

Gemäss dem Projektorganigramm rapportieren die Qualitätssicherung (QS) und das Risikomanagement (RM) direkt an den Projektleiter und nicht wie in der «Weisung des Bundesrates für IKT-Schlüsselprojekte» vom 27. März 2013 gefordert an den Projektauftraggeber.

Gemäss den AKV berät und unterstützt der PA den PAG und besitzt nur Empfehlungskompetenzen, einzig der Projektauftraggeber besitzt Entscheidungskompetenzen. Aus den Projektausschussprotokollen geht hervor, dass die bisherigen Projektsteuerungsentscheide durch das Gremium «Projektausschuss» getroffen wurden. Nach Auskunft des PAG wurde die Entscheidungsfindung im Gremium bewusst gewählt. Die Gesamtverantwortung verbleibt weiterhin beim PAG.

Beurteilung

Aus Sicht der EFK ist das Projekt klar strukturiert, die Rollen und Zuständigkeiten sind, gemäss HERMES 5 definiert und im PM-Plan dokumentiert. Die Unterstellung des QS/RM müsste entsprechend der «Weisung des Bundesrates für IKT-Schlüsselprojekte» sowie im Sinne der unabhängigen Beurteilung und Berichterstattung, direkt dem PAG unterstellt sein.

Mit der Bestimmung des Generalsekretärs zum PAG, wurde aus Sicht der EFK zweckmässig auf die Situation (Abbruch ISS 1) reagiert. Die Zusammensetzung des PA ist stufengerecht und die Anzahl der Mitglieder ist angemessen. Durch die Einbindung des ISS 2 in die wöchentliche GL-Sitzung im ISC-EJPD erhält das Projekt zudem die notwendige Managementattention, um allfällige Projektanliegen und/oder -probleme direkt und schnell behandeln zu können.

Die den beiden Teilprojekt-Auftraggebern zugewiesenen AKV entsprechen grundsätzlich denen des PAG, jedoch explizit für ihre Verantwortungsbereiche. Damit ergeben sich aus Sicht der EFK keine Widersprüche oder Unklarheiten bezüglich der Entscheidungskompetenzen im Projekt. Diese verbleiben vollständig beim PAG. Durch die Gremienentscheide im Projektausschuss werden die Kompetenzvorgaben nicht eingehalten.

Empfehlung 1 (Priorität 1):

Die EFK empfiehlt dem Generalsekretär EJPD in seiner Rolle als Projektauftraggeber, sicherzustellen, dass

- *ihm das Qualitäts- und Risikomanagement direkt unterstellt wird und das Projektorganigramm und der PM-Plan entsprechend nachgeführt werden.*
- *künftige Projektsteuerungsentscheide entsprechend den Kompetenzvorgaben getroffen werden.*

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:

Die Empfehlung wird angenommen, das Projektorganigramm angepasst. Der Einbezug des PA bei den Projektsteuerentscheiden wird insofern nicht geändert als einigen PA-Mitgliedern die Rolle eines Teil-Projektauftraggebers zukommt, wobei die Schlussverantwortung beim PAG liegt.

3.2 Die Projekteinführung ist aktuell nicht gefährdet

Die Terminplanung ist über Meilensteine definiert, welche mit dem Lieferanten vertraglich vereinbart wurden und im PM-Plan abgebildet sind. Die Meilensteine werden im Masterplan in Bezug auf den Vertrag, Produktivumgebung, Projektplanung, Einführung, offene Entscheide und Projektphasen abgebildet. Mit dem Masterplan und dem darauf aufbauenden Statusbericht wird der Projektausschuss monatlich über die Projektentwicklung informiert.

Im Auftragsmanagement-Tool „JIRA“ werden auf Stufe der Komponenten (HERMES-Module) die Meilensteine mit den sogenannten Versionen übernommen und auf die einzelnen Aufträge heruntergebrochen. Über eine Schnittstelle werden die JIRA-Termindaten ins MS-Project importiert und dort in der Feinplanung abgebildet. Auf dieser Planungssicht erfolgt die Überwachung der Meilensteine. Ein kritischer Pfad für die Überwachung der Terminabhängigkeiten ist nicht erstellt. Gemäss der heutigen Terminplanung und dem aktuellen Projektstand geht die Projektleitung davon aus, dass der Produktivstart von ISS 2 im März 2015 nicht gefährdet ist.

Über die Projekt-Ressourcenmanagement-Lösung „PROTOS“ werden, jeweils bezogen auf das Kalenderjahr, die monatlich benötigten Personalressourcen in Form von Rollen (Bsp. Betrieb, Integration, Netz, ÜPF) und Personentagen (PT) bei den zuständigen Bereichen angefragt. Die zugesicherten Personentage gelten als verfügt und die Mitarbeiterinnen und Mitarbeiter werden fachlich durch den PL geführt. Über das PROTOS werden auch die Kostenstellen, auf welche die Mitarbeiterinnen und Mitarbeiter über die Leistungserfassung „CATS“ abrechnen, auf das Projekt ISS 2 verlinkt.

Beurteilung

Die definierten Meilensteine weisen einen zeitlichen Abstand in der Grössenordnung von einem Monat auf, was aus Sicht der EFK eine vernünftige Zeitspanne für die Terminüberwachung darstellt und mit der Berichterstattung an den PA korrespondiert. Zudem wurden mit dem Masterplan und Statusbericht geeignete Instrumente aufgebaut um den PA über die Projektentwicklung zu informieren.

Mit PROTOS besitzt das ISC-EJPD ein Instrument, welches die Personalressourcenplanung pragmatisch unterstützt. Die EFK beurteilt es positiv, dass die intern erbrachten Eigenleistungen

(Zeit pro Person) erfasst und auf das Projekt abgerechnet werden. Damit wird die Transparenz im Projekt verbessert.

3.3 Aus heutiger Sicht ist die Finanzierung des Projekts ISS 2 gesichert

Der aktuelle Verpflichtungskredit beträgt 31,2 Millionen Franken und setzt sich aus dem Kredit für ISS 1 (18,2 Millionen Franken, wobei verschiedene Investitionen in die das Kern-System umgebende Infrastruktur für ISS 2 weiterverwendet werden können) und dem Zusatzkredit für ISS 2 (13,0 Millionen Franken) zusammen. Der Zusatzkredit wurde mit Bundesbeschluss[2] am 3. Dezember 2013 genehmigt. Nach Abrechnung des Projektes ISS 1 ergibt sich ein nicht beanspruchter Kreditanteil von 1,2 Millionen Franken. Zusammen mit dem Zusatzkredit ergibt sich für ISS 2 ein Kreditrest von 14,2 Millionen Franken.

Im Bericht Konzept ISS 2 (Version 1.0 vom 19. Mai 2014) wird mit Bezug auf den «finanziellen Status - Gesamtübersicht» ein positiver Saldo an finanzwirksamen Mitteln in der Höhe von 0,3 Millionen Franken ausgewiesen. Weiter wird erwähnt, dass zusätzliche Mittel frei werden könnten.

3.4 Das Controlling ist angemessen, das PCOE wird nicht angewendet

Zentrales Instrument für das finanzielle Projektcontrolling und die Vertragsüberwachung ist die durch das Projektoffice aufgebaute und geführte Excel «ISS 2_Buchhaltung_A». Die Ist-Kosten werden aus dem SAP laufend, manuell übernommen und mit dem Projektbudget verglichen. Monatlich wird der finanzielle Status für den PA erstellt. Ergänzend wird durch den Bereich Finanzen des ISC-EJPD halbjährlich das Verpflichtungskredit-Controlling zuhanden der EFV erstellt.

Das in der «Weisung des Bundesrates für IKT-Schlüsselprojekte» vom 27. März 2013 geforderte erweiterte Projektcontrolling (PCOE) wird noch nicht angewendet.

Beurteilung

Das für das Projektcontrolling verwendete Excel-Instrument macht aufgrund der schlanken Projektbudgetstruktur und der Tatsache, dass der Lieferantenvertrag rund 75% der Projektbudgets ausmacht und mit einem Zahlungsplan hinterlegt ist, einen angemessenen Eindruck. Bezüglich der Anwendung des PCOE sind die Vorgaben in der Weisung des Bundesrates für IKT-Schlüsselprojekte eindeutig und dementsprechend umzusetzen.

Empfehlung 2 (Priorität 2):

Die EFK empfiehlt dem Generalsekretär des EJPD in seiner Rolle als Projektauftraggeber sicherzustellen, dass das erweiterte Projektcontrolling (PCOE) beim Projekt ISS 2 entsprechend den Vorgaben angewendet wird.

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:
Die Empfehlung wird angenommen. Der PCOE Bericht wird ab der nächsten ordentlichen Berichterstattung erstellt.

[2] Bundesbeschluss I über den Nachtrag II zum Voranschlag 2013 vom 3. Dezember 2013

3.5 Risiko- und Massnahmenverantwortung sind nicht bezeichnet

Gemäss dem PM-Plan basiert das Risikomanagement auf den Vorgaben aus HERMES 5. Auf Ebene des Projektes werden die Ergebnisse des Risikomanagements in einem Risikokatalog dokumentiert. Nach Auskunft des Projektoffice, wird die Risikosituation seit kurzem im Kernteam besprochen, gegebenenfalls nachgeführt und protokolliert. Der Risikokatalog wird monatlich nachgeführt. Aus ihm geht nicht hervor, wer für die einzelnen Risiken und Massnahmen die Verantwortung trägt.

Mit dem Statusbericht, der die Struktur des Masterplans übernimmt, wird der Projektausschuss monatlich je Thema (Bsp. Vertrag, Produktivumgebung, Projektplanung etc.) mit Ampelbewertungen über die Projektentwicklung informiert. Dabei wird der Statusbericht mit ausgewählten Risiken aus dem Risikokatalog, welche bei der Übernahme in den Statusbericht neu bewertet werden, ergänzt. Die Auswahl der Risiken und die Neubewertung erfolgt gemeinsam durch den Projektleiter und das Projektoffice. Gemäss Auskunft des PL hat sich der PA bewusst entschieden auf den Risikokatalog Stufe Projekt zu verzichten.

Beurteilung

Gemäss der «Weisungen des Bundesrates für IKT-Schlüsselprojekte» ist der Projektauftraggeber Eigner der Risiken aus IKT-Schlüsselprojekten. Aus Sicht der EFK ist diese Ownerschaft übergeordnet zu verstehen und ersetzt nicht die operative Verantwortung für ein Risiko und der dazugehörigen Massnahmenumsetzung. Diese operative Verantwortung (Risiko- und Massnahmenverantwortung) ist im Risikokatalog wie vorgesehen einzupflegen, ansonsten besteht die Gefahr, dass sich niemand für das Risiko verantwortlich fühlt und sich die Eintretenswahrscheinlichkeit erhöht.

Empfehlung 3 (Priorität 1):

Die EFK empfiehlt dem Generalsekretär des EJPD in seiner Rolle als Projektauftraggeber sicherzustellen, dass je Risiko und dazugehöriger Massnahmen die operative Verantwortung definiert wird.

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:
Die Empfehlung wird angenommen. Der Risikokatalog wurde bereits erweitert und die Zuweisung der verantwortlichen Rollen ist im Gange.

4 Lösungsumsetzung

4.1 Die Lösungsarchitektur unterstützt die Zielsetzung von ISS 2 und architekturbedingte Einschränkungen sind von den Stakeholdern akzeptiert

Durch das Lenkungsgremium FMÜ wurden folgende Rahmenbedingungen für ISS 2 festgelegt und die entsprechenden Einschränkungen ausdrücklich akzeptiert:

- Mit ISS 2 wird ein Basis-System bereitgestellt, welches auf einer Standardlösung basiert und einzig diejenigen Anforderungen umsetzt, die für eine lauffähige Lösung notwendig sind
- Das Basis-System wird nicht (standort-) redundant betrieben
- Es wird ein Integrations- und ein Produktiv-System betrieben, jedoch kein Test-System. Test von Patches und Weiterentwicklungen, sowie Schulungen sollen auf dem Integrationssystem durchgeführt werden

Das Basis-System (Kernsystem und Delta A) wird vom Lieferanten als Blackbox-System (Hardware und Software) geliefert, installiert und konfiguriert. Entsprechend hat das ISC-EJPD nur beschränkten Einfluss auf die verbauten Technologien.

Teile der Zugriffsnetze für die Strafverfolgungsbehörden müssen aufgrund der gestiegenen Anforderungen durch ISS 2 ausgebaut werden. Die diesbezüglichen Arbeiten sind initiiert, liegen aber nicht alle im Einflussbereich des EJPD.

Der Eingangsbuffer[3] ist die zentrale Massnahme zur Sicherstellung der Verfügbarkeit bei zu hoher Dateneinleitung von den FDA, bei Wartung oder Ausfällen des ISS 2 Basis-Systems oder im Katastrophenfall. Zum Prüfungszeitpunkt lag das Konzept des Eingangsbuffers nur im Entwurf vor. Gemäss Konzept wird der Eingangsbuffer standortübergreifend redundant ausgelegt, jeweils mit eigenem Speicher. Aktuell besteht eine temporäre Eigenentwicklung des Eingangsbuffers vom ISC-EJPD für Testzwecke in der Integrationsumgebung, welche zur Simulation des Eingangsbuffers dient jedoch nicht alle Anforderungen an die endgültige Lösung abdecken kann. Zum Zeitpunkt der Prüfung war noch nicht entschieden, ob der produktive Eingangsbuffer weiter auf einer Eigenentwicklung basieren oder in einer WTO als Gesamtlösung ausgeschrieben werden soll.

Die IP-Überwachung ist ein neuer Bereich mit vielen Herausforderungen in einem dynamischen Umfeld mit rasanter technologischer Entwicklung und nicht abschätzbaren Kapazitätssteigerungen auf Seiten der FDA. Die Berechnungen für die Dimensionierung der Systeme und der Netze basieren auf Annahmen, Lieferanten-Angaben und Vergangenheitswerten, welche in die Zukunft extrapoliert wurden.

Um den Aspekten des Business Continuity Management gerecht zu werden ist vorgesehen, im Katastrophenfall das Integrations- zu einem Produktions-System umzubauen. Dieses Vorgehen

[3] Der Eingangsbuffer ist ein System, welches Überwachungsdaten (nur „packet switched“ [PS]) und Metadaten von Überwachungen (PS und „circuit switched“ [CS]) aufnimmt, zwischenspeichert und bei Systemverfügbarkeit weiterleitet, wenn das ISS System diese aufgrund seiner maximalen Verarbeitungskapazität nicht mehr direkt aufnehmen kann.

nimmt ca. 2-3 Wochen in Anspruch und es ist mit einem teilweisen Verlust der eingeleiteten Daten zu rechnen. Dieses Risiko ist den Stakeholdern bekannt und wird von ihnen akzeptiert.

Beurteilung

Der Vorteil am Blackbox-Ansatz ist der Umstand, dass Software und Hardware optimal aufeinander abgestimmt sind, beides in der Verantwortung des Lieferanten liegt und der Support damit sichergestellt ist. Hingegen hat das ISC-EJPD nur eine begrenzte Kontrolle über die Sicherheitsmassnahmen innerhalb des Kernsystems und nur geringen Einfluss auf den Lifecycle-Rhythmus.

Der Eingangsbuffer ist zentral für die Verfügbarkeit des Systems, die Katastrophenvorsorge und die Sicherstellung der Entgegennahme von Daten seitens FDA. Für die EFK erhöht das Fehlen des Buffer-Konzepts das generelle Risiko für Datenverluste.

Die Zahlen, welche der Dimensionierung von System- und Netzkapazitäten zugrunde liegen, sind nicht erhärtet und stellen ein Betriebsrisiko dar. Ein allfälliger Ausbau der Kapazität bedingt eine vertiefte Analyse jeder einzelnen Komponente in der Verarbeitungskette und ist somit nicht ohne Vorlaufzeit realisierbar.

Empfehlung 4 (Priorität 1):

Die EFK empfiehlt dem ISC-EJPD sicherzustellen, dass die Konzeption des Eingangsbuffers entsprechend seiner Priorität im Projekt vorangetrieben und der Entscheid bezüglich Eigenentwicklung oder Ausschreibung getroffen wird.

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:

Die Empfehlung wird im Grundsatz akzeptiert. Wir weisen aber darauf hin, dass die Konzipierung und Umsetzung des Buffers mit tieferer Priorität vorangetrieben wird um die termingerechte Einführung von ISS 2 nicht zu gefährden. Mit folgendem Hintergrund:
Nach wie vor droht bei einem Ausfall des bestehenden veralteten Systems ein Totalausfall der Telekommunikationsüberwachung.
Das ISS wäre auch ohne einen Eingangsbuffer voll funktionsfähig und könnte system-immanent kurzfristige Überschreitungen der Einleitungskapaziät abfangen.
Der aktuell eingesetzte temporäre Buffer ist in die laufenden Tests integriert und gibt zusätzliche Sicherheit.

Empfehlung 5 (Priorität 1):

Die EFK empfiehlt dem ISC-EJPD die effektiven Dateneinleitungsvolumen ab Produktionsstart systematisch zu überwachen und mit den Dimensionierungsgrundlagen abzugleichen. Weiter sollten bereits im Vorfeld der Betriebsphase die Pläne für einen allfälligen Systemausbau bei unterschiedlichen Bedarfssituationen vorbereitet werden.

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:

Wir stimmen der inhaltlichen Aussage der Empfehlung zu und leiten die notwendigen Massnahmen ein. Voraussetzung ist aber, dass die für den Ausbau notwenigen Mittel auch gesprochen werden.

Empfehlung 6 (Priorität 1):

Die EFK empfiehlt dem ISC-EJPD, noch vor Produktivsetzung von ISS 2 detaillierte Notfallpläne mit Drehbüchern zu erstellen.

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:
Die Empfehlung wird akzeptiert. Das Erstellen der notwendigen Notfallpläne ist Bestandteil des Betriebshandbuches.

4.2 Der Schutzbedarf ist ermittelt, das Sicherheitskonzept steht noch aus

Der Schutzbedarf von ISS 2 wurde analysiert und in der Schutzbedarfsanalyse festgehalten. ISS 2 ist mit den Sicherheitsweisungen des Bundes nur begrenzt kompatibel, daher wurden viele Ausnahmegenehmigungen notwendig, welche bei den verantwortlichen Stellen beantragt und von diesen genehmigt wurden.

Ende Juni 2014 lag das ISDS-Konzept für ISS 2 im Entwurf vor. Die Erarbeitung ist im Verzug. Nach den HERMES-Vorgaben hätte das Sicherheitskonzept bereits beim Phasenübergang vom Konzept zur Realisierung von ISS 2 genehmigt werden müssen. Durch die fehlende Genehmigung sind die ausgewiesenen Restrisiken formell nicht durch den PAG akzeptiert.

Beurteilung

Die Schutzbedarfsanalyse ist aus Sicht der EFK nachvollziehbar. Durch die verspätete Erstellung und Genehmigung des Sicherheitskonzeptes besteht das Risiko, dass allfällige Auflagen das Projekt terminlich und kostenmässig beeinflussen können und Nachbesserungen an technischen und/oder betrieblichen Konzepten notwendig werden. Es bleibt eine grosse Anzahl an Restrisiken bestehen, welche noch nicht durch die notwendigen Instanzen akzeptiert sind.

Empfehlung 7 (Priorität 1):
Die EFK empfiehlt dem ISC-EJPD, das Sicherheitskonzept (ISDS) mit hoher Dringlichkeit zu erarbeiten, genehmigen zu lassen und allfällige Sicherheitsauflagen umzusetzen.

Stellungnahme des Eidgenössischen Justiz- und Polizeidepartements:
Die Empfehlung wird angenommen. Dies umso mehr, als die Bearbeitung derzeit mit hoher Dringlichkeit erfolgt.

4.3 Die Konzeption der Einführung mit Migration und Tests ist auf gutem Weg

Für die Systemablösung wurde ein Migrationskonzept erstellt. Das bisherige System LIS wird parallel betrieben, bis sämtliche darauf laufenden Massnahmen beendet sind. Alle neuen Überwachungsmassnahmen werden ab Produktionsstart auf das neue ISS System geschaltet.

Das Testkonzept liegt in einer genehmigten Version (1.0 vom 15. Mai 2014) vor. In der aktuellen Version (1.1 vom 13. Juni 2014) hat es noch Lücken im Bereich Accounts und Zugriffe sowie bei der detaillierten Testplanung. Die Detail-Konzepte und Drehbücher für die Tests sowie die Testcases sind derzeit in Erarbeitung.

Beurteilung

Die im Migrationskonzept beschriebenen Schritte werden von der EFK als zielführend beurteilt.

Das Testkonzept ist, dem aktuellen Stand entsprechend, bis auf wenige Lücken vollständig und anwendbar. Diese werden noch vor Testbeginn beseitigt. Die Testcases sind entscheidend für die erfolgreiche Einführung. Sie werden daher im Risikomanagement geführt und erhalten die notwendige Aufmerksamkeit.

4.4 Der Betrieb von ISS 2 ist mit Unsicherheiten bezüglich Kapazitäten behaftet

Die Massnahmen für die Einbindung von ISS 2 in die bestehende Betriebsorganisation des ISC-EJPD sind geplant und in Umsetzung. Das Betriebskonzept ist in Arbeit. Die Integrations-Plattform im ISC-EJPD ist aufgebaut und der Aufbau der Produktions-Plattform ist leicht im Verzug, jedoch ohne terminliche Konsequenzen für andere Aufgaben. Die Schulungen der Betriebsmannschaft sind geplant.

Die im Bereich Lösungsarchitektur (Kapitel 4.1) beschriebenen Herausforderungen im Zusammenhang mit dem Eingangsbuffer, der Dimensionierung von System und Netzen sowie die Erarbeitung der Notfallpläne betreffen in hohem Masse auch den Betrieb von ISS 2.

Aufgrund der fehlenden (Standort-)Redundanz von ISS 2 kann der Service Level «Platin» des ISC-EJPD nicht gewährleistet werden. Hier muss ein spezielles Organisation Level Agreement (OLA) zwischen Betrieb & Support und dem Dienst ÜPF ausgehandelt werden. Laut Planung soll dieser Task mit Abschluss der Phase Einführung erledigt sein.

Beurteilung

Der Aufbau der Integrations- und Produktions-Plattformen ist im Plan und die notwendigen Handbücher und Konzepte sind im Aufbau oder werden vom Hersteller geliefert. Die Schulungen wie auch die Erstellung des OLA sind geplant. Die Eingliederung in die bestehenden Betriebs- und Support-Prozesse ist geplant und die AKV sind definiert. Das Bewusstsein für (Zugriffs-) Sicherheitsthemen im Betrieb, insbesondere im Zusammenhang mit dem Blackbox-System ist vorhanden. Damit sind aus Sicht EFK die Voraussetzungen für eine erfolgreiche Betriebseinführung gegeben.

Dass ISS 2 lediglich aus einem Produktions- und einem Integrations-System besteht, welche beide nicht redundant ausgelegt sind, bringt grosse Herausforderungen für den Betrieb mit sich. Dies betrifft vor allem die Zuständigkeiten und Zeitzuteilungen auf dem Integrationssystem. Noch nicht detailliert geplant ist das Vorgehen bei Notfallsituationen. Entsprechende Empfehlungen finden sich im Kapitel 4.1.

5 Beschaffung

Die Beschaffung des ISS 1-Systems erfolgte gestützt auf BöB Art. 3 im Einladungsverfahren, wonach Aufträge nicht nach den Bestimmungen des Beschaffungsgesetztes vergeben werden müssen, wenn dadurch die öffentliche Ordnung und Sicherheit gefährdet sind.

Nachdem absehbar wurde, dass das Projekt ISS 1 mit dem gewählten Lieferanten nicht erfolgreich abgeschlossen werden konnte, hat das Lenkungsgremium FMÜ im März 2013 die relevanten Stakeholder beauftragt, das System des heutigen Lieferanten zu evaluieren. Nach dem Entscheid zum Projektabbruch ISS 1 im September 2013 konnten mit dem Lieferanten direkt Vertragsverhandlungen aufgenommen werden. Die Vertragsunterzeichnung zwischen dem ISC-EJPD und dem Lieferanten fand im Dezember 2013 statt. Der Vertrag beinhaltet einen Zahlungsplan (30/30/30/10) und aufgrund des fehlenden Wettbewerbs wurde ein Einsichtsrecht vereinbart. Die erste Zahlung erfolgte zum Zeitpunkt der Vertragsunterzeichnung und wurde durch eine Bankgarantie vollumfänglich abgesichert.

Im Beschaffungsplan für ISS 2 nicht enthalten, jedoch im Projektbudget berücksichtigt ist die Beschaffung des Eingangsbuffers (siehe auch Kapitel 5.1).

Beurteilung

Der heutige Lieferant hat bereits das System LIS gebaut und kann daher als einziger den notwendigen Support für dieses System bis zum Projektende von ISS 2 gewährleisten. Vor diesem Hintergrund ist die Beschaffung beim heutigen Lieferanten für ISS 2 für die EFK nachvollziehbar.

Weiter bewertet es die EFK positiv, dass vertraglich ein Einsichtsrecht in die Kalkulation des Lieferanten gemäss Verordnung über das öffentliche Beschaffungswesen (VöB) Art. 5 sowie die Möglichkeit von externen Audits vereinbart wurde und die erste Tranche des Zahlungsplans, im Sinne einer Vorauszahlung, mit einer Bankgarantie abgesichert wurde. Durch das Einsichtsrecht ist die Möglichkeit gegeben, dass trotz starker Lieferanten-Bindung ein gewisser Einfluss auf die Kosten von allfälligen Weiterentwicklungen gewahrt werden kann.

Sollte eine öffentliche Beschaffung (WTO) des Eingangsbuffers notwendig werden, so wird er zur geplanten Produktivsetzung des Systems mit grosser Wahrscheinlichkeit nicht verfügbar sein. Für diesen Fall besteht zwar ein Szenario, wonach der temporäre Eingangsbuffer, welcher zum Zweck der Testbarkeit der Integrationsumgebung gebaut wurde, ausgebaut und produktiv eingesetzt wird.

6 Schlussbesprechung

Die Schlussbesprechung fand am 28. Juni 2014 statt. Teilgenommen haben Matthias Ramsauer und Stefan Jost, GS-EJPD; Christian Baumann, Heiner Peters und René Koch, ISC-EJPD. Die EFK war vertreten durch Michel Huissoud, Roland Bosshard und Martin Schwaar.

Sie ergab Übereinstimmung mit den wesentlichen Feststellungen und Empfehlungen.

Die EFK dankt für die gewährte Unterstützung.

Die Finanzdelegation der eidgenössischen Räte hat an ihrer ordentlichen Sitzung im September 2014 vom Bericht Kenntnis genommen.

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen, Priorisierung der Empfehlungen

Rechtsgrundlagen:

Finanzkontrollgesetz (FKG, SR 614.0)

Finanzhaushaltgesetz (FHG, SR 611.0)

Finanzhaushaltverordnung (FHV, SR 611.01)

Bundesinformatikverordnung (BinfV, SR 172.010.58)

Priorisierung der Empfehlungen:

Die EFK beurteilt die Wesentlichkeit der Empfehlungen nach Prioritäten (1 = hoch, 2 = mittel, 3 = klein). Sowohl der Faktor Risiko (z.B. Höhe der finanziellen Auswirkung, Wahrscheinlichkeit eines Schadeneintrittes usw.) als auch der Faktor Dringlichkeit der Umsetzung (kurzfristig, mittelfristig, langfristig) werden berücksichtigt. Dabei bezieht sich die Bewertung auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

Anhang 2: Abkürzungen

Abkürzungen:

AKV	Aufgaben, Kompetenzen und Verantwortung
BCM	Business Continuity Management
BöB	Bundesgesetz über das öffentliche Beschaffungswesen
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
CS	Circuit Switched
FDA	Fernmeldedienst-Anbieterin
FMÜ	Fernmeldeüberwachung
IP	Internet Protokoll
ISC	Informatik Service Center
ISDS	Informationssicherheit und Datenschutz
ISS	Interception System Schweiz
ITSCM	IT Service Continuity Management
KAPO BE	Kantonspolizei Bern
KKPKS	Konferenz der kantonalen Polizeikommandanten
LG FMÜ	Lenkungsgremium Fernmeldeüberwachung
LIS	Lawful Interception System
OLA	Organisation Level Agreement
PA	Projektausschuss
PAG	Projekt-Auftraggeber
PCO	Projekt-Controlling
PCOE	Erweitertes Projekt-Controlling
PS	Packet Switched
PT	Personentage
QS	Qualitätssicherung
RM	Risikomanagement
SLA	Service Level Agreement
ÜPF	Überwachung Post- und Fernmeldeverkehr
VöB	Verordnung über das öffentliche Beschaffungswesen
WTO	World Trade Organization