Seattle Information Technology

2023 Surveillance Impact Report

Hostage Negotiation Throw Phone: Executive Overview

Seattle Police Department

#	Ordinance Section	Requirement	SIR Section/Policy
	14.18.040.B.1	A description of the surveillance technology to be acquired	**1.0 Abstract /2.0 Technology Overview** The hostage negotiation throw phone is a phone in a hardened case that is part of a communications system for use in police hostage/crisis negotiations with subjects. The phone case includes microphones and speakers to enable two-way communication in an overt or covert manner. It also includes hidden cameras to support threat and tactical assessments. At times there are no other means of phone communication with the subject in a hostage or barricaded person situation and this system allows for safe and reliable communication from a distance. The system allows the team monitoring and recording of conversations to facilitate the development of negotiation strategies and ensure the safety-related information is relayed.
1		Description of the general capabilities	**1.1 Abstract /2.3 Technology Overview** The hostage negotiation throw phone is a phone in a hardened case that is part of a communications system for use in police hostage/crisis negotiations with subjects. The phone case includes microphones and speakers to enable two-way communication in an overt or covert manner. It also includes hidden cameras to support threat and tactical assessments.

			The hostage negotiation throw phone is a phone in a hardened case that is part of a communications system for use in police hostage/crisis negotiations with subjects. The phone case includes microphones and speakers to enable two-way communication in an overt or covert manner. It also includes hidden cameras to support threat and tactical assessments.
2		The type of data that the technology is reasonably likely to generate	**1.1 Abstract**
3		functionality, including reasonably foreseeable surveillance capabilities outside the scope of the City department's proposed use.	**1.2 Abstract** This system is intended to provide a reliable means of communication between a hostage taker or barricaded subject and police hostage negotiators. At times there are no other means of phone communication with the subject and this system allows for safe and reliable communication from a distance. The system allows the SPD team monitoring and recording conversations to facilitate the development of negotiation strategies and ensure the safety- related information is relayed. In addition to the overt communication capabilities, this technology also captures images and audio of identifiable individuals, some of whom are unaware of the recording. Without appropriate safeguards, this raises significant privacy concerns.

	14.18.040.B.2	A description of the purpose and proposed use of the surveillance technology, including, if available	**2.1 Technology overview** At times there are no other means of phone communication with the subject in a hostage or barricaded person situation and this system allows for safe and reliable communication from a distance. The system allows the team monitoring and recording of conversations to facilitate the development of negotiation strategies and ensure the safety-related information is relayed.
4		Intended benefits of the applicable surveillance technology	**2.1 Technology overview** The system allows the team monitoring and recording of conversations to facilitate the development of negotiation strategies and ensure the safety-related information is relayed.
5		Any data or research demonstrating those benefits.	**2.2 Technology overview / Expertise and References** Throw phone systems of this nature are standardized equipment for Hostage/Crisis Negotiation Teams according to the National Council of Negotiation Associations, FBI Crisis Negotiation Unit, National Tactical Officers' Association, and other industry standards. Approximately 15 years ago, the industry standard for these systems began to include video monitoring capabilities. Such monitoring capabilities were

			deemed important to be able to assess the demeanor of the subject and whether there were any life-safety factors present such as the injured parties or threats of violence.
	14.18.040.B.3	A clear use and data management policy, including protocols for the following:	**3.0 Use Governance** The equipment is stored on the HNT truck and can only be accessed by HNT or SWAT team members. If it is prepared for use or deployed on an incident its use is logged on the HNT after-action report. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Delivery of the throw phone is typically pre-negotiated with the subject via hailing or other means. For delivery of the throw phone to the subject it is typically brought to the outside of a door or balcony by SWAT team members and the subject is asked to bring it inside for use. It may also be delivered by a large remotely controlled robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door.
6	**14.18.040.B.3.d**	How and when the surveillance technology will be deployed or used by whom, including but not limited to:	**2.5 Technology overview** The equipment is stored on the HNT truck and can

			only be accessed by HNT or SWAT team members. If it is prepared for use or deployed on an incident its use is logged on the HNT after-action report. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Delivery of the throw phone is typically pre-negotiated with the subject via hailing or other means. For delivery of the throw phone to the subject it is typically brought to the outside of a door or balcony by SWAT team members and the subject is asked to bring it inside for use. It may also be delivered by a large remotely controlled robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door.
7		The factors that will be used to determine where, when, and how the technology is deployed;	**2.5 Technology overview/ 3.1 Use Governance** The equipment is stored on the HNT truck and can only be accessed by HNT or SWAT team members. If it is prepared for use or deployed on an incident its use is logged on the HNT after-action report. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Delivery of the throw phone is typically pre-

			negotiated with the subject via hailing or other means. For delivery of the throw phone to the subject it is typically brought to the outside of a door or balcony by SWAT team members and the subject is asked to bring it inside for use. It may also be delivered by a large remotely controlled robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door. Deployment into a constitutionally protected area requires an authorized entry into the area via warrant or warrant exception to include consent, exigent circumstances, or community caretaking/emergency. RCW 9.73.030 expressly provides an exception to the "all parties" consent rule for the monitoring, intercepting, and recording of calls involving communications with a hostage holder or barricaded person.
8		other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances,	**4.4/4.5 Data Collection and Use** The throw phone system is rarely utilized. Of the 168 incidents that HNT responded to in 2021 the throw phone portion of the system was only prepared for delivery a handful of times but was not deployed.
9		whether the technology will be installed permanently or temporarily,	**4.5 Data Collection and Use**

			Temporary deployment only.
10		If the technology is a physical object visible to the public,	**4.6 Data Collection and Use** The throw phone is a physical device in a hardened case connected to a console located with SPD negotiators. The delivered portion of the throw phone does not contain identifying labels or markings.
11		a description of markings that will be used and	**4.6 Data Collection and Use** The throw phone is a physical device in a hardened case connected to a console located with SPD negotiators. The delivered portion of the throw phone does not contain identifying labels or markings.
12		how they will be placed in order to clearly and visibly identify the responsible department and contact information,	**4.6 Data Collection and Use** **N/A**
13		or else an explanation of why such markings would render the surveillance ineffective.	**4.6 Data Collection and Use** **N/A**
14		If the surveillance technology will be operated or used by another entity on the City's behalf, the SIR must explicitly include a description of the other entity's access and any applicable protocols.	**4.8 Data Collection and Use /6.4 Data Sharing and Accuracy** **N/A**

15	**14.18.040.B.3.b**	Any additional rules that will govern use of the surveillance technology	**3.2 Use Governance / 7.1 Legal Obligations, Risks and Compliance** Deployment into a constitutionally protected area requires an authorized entry into the area via warrant or warrant exception to include consent, exigent circumstances, or community caretaking/emergency. RCW 9.73.030 expressly provides an exception to the "all parties" consent rule for the monitoring, intercepting, and recording of calls involving communications with a hostage holder or barricaded person.
16		what processes will be required prior to each use of the surveillance technology, including but not limited to:	**3.1 Use Governance** The equipment is stored on the HNT truck and can only be accessed by HNT or SWAT team members. If it is prepared for use or deployed on an incident its use is logged on the HNT after-action report. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Delivery of the throw phone is typically pre-negotiated with the subject via hailing or other means. For delivery of the throw phone to the subject

			it is typically brought to the outside of a door or balcony by SWAT team members and the subject is asked to bring it inside for use. It may also be delivered by a large remotely controlled robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door.
17		what legal standard, if any, must be met before the technology is used, such as for the purposes of a criminal investigation supported by reasonable suspicion.	**3.2 Use Governance** The equipment is stored on the HNT truck and can only be accessed by HNT or SWAT team members. If it is prepared for use or deployed on an incident its use is logged on the HNT after-action report. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Delivery of the throw phone is typically pre-negotiated with the subject via hailing or other means. For delivery of the throw phone to the subject it is typically brought to the outside of a door or balcony by SWAT team members and the subject is asked to bring it inside for use. It may also be delivered by a large remotely controlled robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door.

18	**14.18.040.B.3.c**	How surveillance data will be securely stored. Such methods must allow for the department personnel and any entity performing an auditing function that has lawful access to search and locate specific data to determine that data were properly deleted, consistent with applicable law.	**5.1 Data Storage, Retention and Deletion** Audio/Video data is saved on the hard drive of the DVR/monitoring system. If fully deployed during an actual incident the recordings are downloaded and submitted into evidence or to detectives. The phone calls are recorded on the laptop running the CINT commander software. Recordings of calls with hostage takers or barricaded subjects are downloaded and submitted into evidence. Copies of recordings are also kept in the HNT folder on SPD's network. Access to this folder is restricted to HNT, Crisis Response Team, and SWAT/Special Services commanders. The purpose of these files is for debriefing, assessment, and training. Evidentiary information is downloaded and uploaded into the evidence storage system or provided directly to investigators.
19	**14.18.040.B.3.d**	How surveillance data will be retained and deleted, including the retention period	**5.2 Data Storage, Retention and Deletion** SPD's Audit Unit can conduct an audit of any SPD system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time. SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28

			CFR Part 23.
20		process for regular deletion after the retention period elapses;	**5.3 Data Storage, Retention and Deletion** PD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence.com and associated with a specific GO Number and investigation. Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other

			misconduct are subject to discipline, as outlined in SPD Policy 5.002. Per the CJIS Security Policy: "5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. 5.8.4 Disposal of Physical Media: Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or

			destruction is witnessed or carried out by authorized personnel."
21		what auditing procedures will be implemented to ensure data are not improperly retained beyond the retention period;	**5.2 Data Storage, Retention and Deletion** SPD's Audit Unit can conduct an audit of any SPD system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time. SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.
22		what measures will be taken to minimize the inadvertent or otherwise improper collection of data; and	**5.3 Data Storage, Retention and Deletion / 8.2 Monitoring and Enforcement** SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic

			evidence. Evidence is submitted to the Evidence.com and associated with a specific GO Number and investigation. Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002. Per the CJIS Security Policy: "5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy

			electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. 5.8.4 Disposal of Physical Media: Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.”
23		how any surveillance data, if identified as improperly collected, will be expeditiously destroyed.	**5.3 Data Storage, Retention and Deletion** SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically

			governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence.com and associated with a specific GO Number and investigation. Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002. Per the CJIS Security Policy: "5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall

			maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. 5.8.4 Disposal of Physical Media: Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel."
24		The SIR shall identify a specific departmental unit that is responsible for ensuring compliance with data retention requirements.	**5.4 Data Storage, Retention and Deletion** Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

25		Retention procedures and policies must be developed in compliance with the requirements of Section 3.122.040.	**4.0 Data Collection and Use**
26	**14.18.040.B.3.e**	How surveillance data will be accessed, including who will be responsible for authorizing access,	**4.7/4.8/4.9 Data Collection and Use** Live-feed video is monitored by HNT or SWAT personnel either from the HNT truck, via a system networked laptop, or through a remote view application in range of the wifi system. All of these viewers have controlled access either by password or by permission having to be granted from the main laptop running the software. Video recorded on the hard drive system is only accessible by HNT members through the DVR system. Downloaded video that is submitted as evidence is accessible only to SPD employees with authorized access per the investigative or evidence system standards. Recordings kept in HNT files are accessible to HNT and Crisis Response Team members as well as SWAT and Special Services commanders. The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Audio or video information collected may be used for follow-up investigation, administrative reviews, and

			HNT debriefings, training, and member assessments.
27		who will be allowed to request access, and	**4.9 Data Collection and Use** The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Audio or video information collected may be used for follow-up investigation, administrative reviews, and HNT debriefings, training, and member assessments.
28		acceptable reasons for requesting access; and	**4.9 Data Collection and Use** The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present. Audio or video information collected may be used for follow-up investigation, administrative reviews, and HNT debriefings, training, and member assessments.

29		what safeguards will be used to protect surveillance data from unauthorized access and	**4.10/8.1 Data Collection and Use** The throw phone system video and covert audio recording are stored on the DVR system secured in the HNT truck. Only HNT and SWAT SPD employees have access to the HNT Truck. The data is then securely input and used on SPD's password-protected network with access limited to authorized users. All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems. SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.
30		to provide an audit trail, such as viewer logging or encryption and access control mechanisms, to the extent such mechanisms exist within the contemplated surveillance technology.	**4.10 Data Collection and Use /8.1 Monitoring and Enforcement** The throw phone system video and covert audio recording are stored on the DVR system secured in

			the HNT truck. Only HNT and SWAT SPD employees have access to the HNT Truck. The data is then securely input and used on SPD's password-protected network with access limited to authorized users. All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems. SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time. The HNT Unit does not disclose information collected by the covert cameras. This information is provided to the requesting Officer/Detective to be included in the requisite investigation file. Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any requests for public disclosure are logged by

			SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.
31	**14.18.040.B.3.f**	Whether a department intends to share access to the surveillance technology or the surveillance data from that surveillance technology with any other entity, including any other City department or non-City entity, and	**6.1 Data Sharing and Accuracy** No person, outside of SPD, has direct access to the data collected with the hostage negotiation throw phone. Data collected with the hostage negotiation throw phone may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Data may be shared with outside entities in connection with criminal prosecutions: • Seattle City Attorney's Office • King County Prosecuting Attorney's Office • King County Department of Public Defense • Private Defense Attorneys • Seattle Municipal Court • King County Superior Court • Similar entities where prosecution is in

			Federal or other State jurisdictions Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request. Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Discrete pieces of the data collected with the hostage negotiation throw phone may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law

			enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018. SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files analyzed by this application.
32		if so, with which entity and how such sharing is necessary for the purpose or purposes for which Council approval is requested; and	**6.2 Data Sharing and Accuracy** Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process. For example, an investigator may send out a photo or description of a homicide suspect in order to find out if another LE agency knows their identity.

			Products developed using this information may be shared with other law enforcement agencies. All products created with the information used in this project will be classified as Law Enforcement Sensitive. Any bulletins will be marked with the following restrictions: LAW ENFORCEMENT SENSITIVE — DO NOT LEAVE PRINTED COPIES UNATTENDED — DISPOSE OF IN SHREDDER ONLY – NOT FOR PUBLIC DISPLAY OR DISTRIBUTION — DO NOT FORWARD OR COPY.
33		what restrictions, if any, the department will place upon the receiving non-City entity's use of such surveillance technologies.	**6.3 Data Sharing and Accuracy**
34		If applicable, the SIR shall include a copy of the department's procedures for ensuring the entity's compliance with this provision.	**6.3 Data Sharing and Accuracy**
35	**14.18.040.B.3.g**	How the department will ensure that all personnel who operate surveillance technology or access its surveillance data are knowledgeable about and able to ensure compliance with the use and data management policy prior to use of the surveillance technology or surveillance data from that surveillance technology.	**3.3 Use Governance** All HNT members are trained on the use and set up of the system upon appointment to the team and refreshed on its use during in-service training. Supervisors and commanding officers are responsible for ensuring compliance with policies. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.
36	**14.18.040.B.4**	A description of any community engagement held and any future community engagement plans,	**RET/Public Engagement Plan**

37		including statistics and demographics on attendees,	**RET/Public Engagement Plan**
38		a compilation of all comments received, and departmental responses given, and	**RET/Public Engagement Plan**
39		departmental conclusions about potential neighborhood and disparate impacts that may result from the acquisition.	**RET/Public Engagement Plan**
40	**14.18.040.B.5**	A description of how the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account; and	**RET/Public Engagement Plan**
41		a mitigation plan.	**RET/Public Engagement Plan**
	14.18.040.B.6	A description of the fiscal impact of the surveillance technology, including	**Fiscal Impact Report**
42		initial acquisition costs;	**Fiscal Impact Report**
43		ongoing operating costs such as maintenance,	**Fiscal Impact Report**
44		licensing,	**Fiscal Impact Report**
45		personnel,	**Fiscal Impact Report**
46		legal compliance,	**Fiscal Impact Report**
47		use auditing,	**Fiscal Impact Report**
48		data retention, and	**Fiscal Impact Report**
49		security costs;	**Fiscal Impact Report**
50		any cost savings that would be achieved through the use of the technology; and	**Fiscal Impact Report**