



City of Caribou, Maine

*Municipal Building
25 High Street
Caribou, ME 04736
Telephone (207) 493-3324
Fax (207) 498-3954
www.cariboumaine.org*

**AGENDA
Caribou City Council
City Council Workshop
Immediately following the Council Meeting
On Monday, February 23, 2015
Caribou City Council Chambers**

1. Shared dispatching between police and fire
2. Utilizing Basic EMTs
3. Cary Medical Center
4. Building Permit Fees
5. Other Areas

Upcoming Meeting Dates:

Regular City Council Meeting March 9, 2015 at 6pm

Regular City Council Meeting March 23, 2015 at 6pm





OFFICE OF THE CITY MANAGER
CARIBOU, MAINE

To: Mayor and Council Members
From: Austin Bless, City Manager, Michael Gahagan, Police Chief, and Scott Susi, Fire Chief
Date: February 23, 2015
Re: Shared dispatching between police and fire

One of the topics brought up in the budget season was to share dispatching for police and fire.

First it should be noted that the fire department does not currently dispatch. 911 calls for medical emergencies go to Penobscot or Houlton depending on how the call is made (cell phone or land line). They dispatch to our department who responds to the call. The dispatcher in Houlton or Penobscot may patch us into the call so the responding crew can be informed of what exactly is going on when they get there.

The dispatch call could come into the Police Department which would then inform the crew on duty and have them respond that way. They do this now when there is no one on in the fire station.

If the Police Department were to take this over it would not save any money, as there would be no way to reduce staff in the fire department.

If the fire department were to dispatch for the police department there are several things that would have to be completed before this could happen. That includes, in no particular order,

- Training for all Fire/Ambulance members to dispatch at police standards. This is 80 hours of training.
- Remodeling of the Fire Department dispatch station to make it secure and up to current FBI CJIS standards.
- Terminal agreements with the department
- All terminals would have to be moved up to the Fire Station

We could possibly eliminate three police positions under this scenario. This could save \$166,722 the first year. However, with that we would lose our jail. We would also have to haul our prisoners down to Houlton, which would add costs of approximately \$30,600. There is more information on that on the following pages.

We would also lose the ability of people to walk into the police station and talk to a police officer. There are some stats on the following pages as to the number of walk-ins. That information was gathered when we explored a joint dispatch with Presque Isle.

In December when the Council voted to put the police officer position in the budget that was proposed to be cut it seemed the Council did not want a reduction in the level of service at the police department. If we did this, it would certainly reduce service levels.

More information compiled by the chief is on the following pages.

INDEX

1. 2014 Overall Activity
2. DMV usage for Caribou PD
3. One month list of lobby walk ins
4. State regulations for METRO
5. Copy of terminal agreements
6. FBI CJIS Security policy
7. Quote for moving terminals to FD
8. County Crime Analysis for 2013
9. Police Employment Data for State of Maine
10. Overview of Caribou PD prisoners for 2012-2014 and estimates to haul prisoners
11. Comparison of dispatch salaries with Presque Isle PD
12. Overview of 2014 sexual/child abuse cases

<u>2014</u>	<u>JAN</u>	<u>FEB</u>	<u>MAR</u>	<u>APR</u>	<u>MAY</u>	<u>JUNE</u>	<u>JULY</u>	<u>AUG</u>	<u>SEPT</u>	<u>OCT</u>	<u>NOV</u>	<u>DEC</u>	<u>TOTAL</u>
COMPLAINTS	1942	2030	2420	2025	2074	2414	2359	2512	2399	2067	2387	2007	26636
M/V ACCIDENTS	38	20	31	18	14	20	22	19	18	21	39	46	306
ESCORTS	1	1	0	3	6	7	4	3	5	5	5	2	42
THEFT COMPLAINTS	14	13	11	23	21	30	34	20	11	17	9	12	215
ANIMAL COMPLAINTS	11	8	5	11	11	24	25	18	11	9	9	11	153
DOMESTIC COMPLAIN	6	8	6	8	12	8	5	6	0	7	5	6	77
BURGLARY COMPLAIN	6	6	2	2	9	3	13	5	2	5	3	1	57
O.U.I.	2	2	4	3	5	5	5	1	1	2	2	4	36
M/V THEFTS	0	1	1	0	4	0	2	2	0	0	0	0	10
MISSING PERSONS	4	3	2	3	0	1	1	3	1	1	20	1	40
JUVENILE COMPLAINT	6	14	3	8	10	3	2	5	8	2	3	2	66
CIVIL COMPLAINTS	1	3	0	0	0	0	0	0	0	55	86	0	145
PROWLER COMPLAIN	0	0	0	0	0	0	1	0	0	0	0	0	1
ASSIST OTHER AGENC	18	24	15	16	26	19	26	23	21	19	16	15	238
ASSAULT ARREST	0	0	1	2	4	5	8	4	2	2	0	0	28
THEFT ARRESTS	3	1	1	2	0	6	4	4	2	6	1	6	36
SPEEDING	11	16	14	9	29	26	32	40	4	7	2	1	191
STOPS/CHECKS M/V	1478	1653	1990	1537	1504	1903	1737	1933	1959	1659	1991	1627	20971
PARKING TICKETS	0	0	0	12	0	0	0	0	0	0	0	0	12
HANDLING PRISONER	43	50	56	54	41	46	61	54	59	54	36	32	586
WARRANT ARRESTS	10	14	13	17	4	6	20	11	6	15	10	3	129
UNLAWFUL SEX. CON	0	0	0	0	3	2	1	1	2	3	0	0	12
GROSS SEX. ASSAULT	0	1	1	0	1	0	2	0	2	0	0	0	7
BUSINESS ALARMS	18	16	13	16	17	12	21	15	19	15	15	18	195
BURGLARY ARRESTS	0	0	0	0	0	1	1	1	1	2	0	2	8

①

Received Time: 10:36:04 01-30-15

View Message Details

METRO STATISTICS: 10:36 30JAN2015
PREVIOUS YEAR: 2013

STATION: CARIPD		--- INPUT COUNTS BY HOUR (TOTAL 19313) ---					
(00)	1171	(06)	608	(12)	546	(18)	618
(01)	997	(07)	466	(13)	705	(19)	654
(02)	714	(08)	587	(14)	1189	(20)	662
(03)	801	(09)	623	(15)	1068	(21)	852
(04)	429	(10)	544	(16)	953	(22)	1525
(05)	677	(11)	606	(17)	689	(23)	1629

		--- OUTPUT COUNTS BY HOUR (TOTAL 70395) ---					
(00)	4083	(06)	1194	(12)	2484	(18)	2873
(01)	3327	(07)	1770	(13)	2513	(19)	2969
(02)	2281	(08)	2483	(14)	3762	(20)	3129
(03)	2150	(09)	2768	(15)	4540	(21)	2479
(04)	1309	(10)	2746	(16)	4345	(22)	4642
(05)	1033	(11)	2790	(17)	3096	(23)	5629

NCIC REPORTS:

ARTICLE FILE:

CA	0	CAA	0	CLA	0	CLAA	0
EA	0	EAA	0	EA-P	0	ELA	0
ELAA	0	LA	0	LAA	0	LLA	0
LLAA	0	MA	0	MAA	0	MLA	0
MLAA	0	QA	2	QAB	0	XA	0
XAA	0	XLA	0	XLAA	0	ZA	0
TOTAL	2						

GUN FILE:

CFG	0	CG	0	CLG	0	CRG	0
EFG	0	EFPG	0	EG	0	EG-P	0
ELG	0	ERG	0	LFG	0	LG	1
LLG	0	MFG	0	MG	3	MLG	1
MRG	0	QG	320	QGB	0	XFG	0
XG	0	XLG	0	XRG	0	ZG	0
TOTAL	325						

III:

DEC	0	DRS	0	EHK	0	LHC	0
MHC	0	QWCH	0	QH	4	QR	3
QWI	0	XHC	0	EHN	0	MRS	0
	0						
TOTAL	7						

LICENSE PLATES:

CL	0	EL	1	EL-A	0	EL-F	0
EL-P	0	LL	0	ML	0	XL	1
TOTAL	2						

MISSING:

CM	0	ED	0	EMD	0	EMDC	0
EME	0	EMEC	0	EMI	0	EMIC	0
EMJ	1	EMJC	0	EMN	0	EMO	1
EMOC	0	EMV	0	EMVC	0	LM	0
MD	0	MM	0	QM	0	XD	0
XM	3	XMN	0				
TOTAL	5						

ORI FILE:

MO	0	QO	7	ZO	0
TOTAL	7				

PROTECTION ORDERS:

CPO	0	CTO	0	EPO	0	ENPO	0
EPOC	0	ETO	0	ETOC	0	MPO	0
MTO	0	QPO	1	XNPO	0	XPO	0
XTO	0						
TOTAL	1						

VEHICLE:

CF	0	CV	1	EF	0	EF-A	0
EF-F	0	EF-P	0	EV	1	EV-A	0
EV-F	0	EV-P	0	LF	0	LV	2
MF	0	MV	2	QV	4611	QVB	0
XF	0	XV	0	ZV	0		
TOTAL	4617						

WANTED:

CT	0	CW	0	EN	0	ENS	0
ET	0	ET-C	0	EW	0	EW-C	0
EWJ	0	EWJC	0	LT	0	LW	0
MW	0	MT	0	QW	6150	QWB	0
XN	0	XNS	0	XT	0	XW	0
ZW	0						
TOTAL	6150						

NLETS REPORTS:

ADMINISTRATIVE:

AA	0	AM	93	SM	0	SON	0
TOTAL	93						

CANADIAN:

CAQ	0	CAR	0	CBQ	0	CBR	0
CFQ	0	CFR	0	CGQ	0	CGR	0
CIQ	0	CIR	0	CSQ	0	CSR	0
UQ	2	UR	0	VQ	11	VR	0
WR	0	XQ	4	XR	0	WQ	2
TOTAL	19						

CRIMINAL HISTORY:

AQ	0	AR	0	CR	0	FQ	60
FR	0	IQ	159	IR	0	SOQ	0
SOR	0						
TOTAL	219						

DMV:

BQ	0	BR	0	DNQ	1091	DNR	0
DQ	1704	DQG	0	DR	0	KQ	0
KR	0	QMP	0	RMP	0	RNQ	325
RNR	0	RQ	131	RQG	0	RR	0
SQ	0	SR	0				
TOTAL	3251						

ORION:

TA	0	TD	0	TQ	14	TR	0
TU	0						
TOTAL	14						

OTHER:

FCC	0	FEC	0	HQ	0	HR	0
IAQ	0	IAR	0	MQ	0	MR	0
NFQ	0	NFR	0	NLQ	0	NLR	0
SWQ	0	SWR	0	YQ	5	YR	1
ACQ	0	ACR	0	AVQ	0	AVR	0
RCQ	0						
TOTAL	6						

STATE DATABASE (SDB) REPORTS:

CONDITION OF RELEASE:

ECOR	143	ENCOR	12	GECOR	0	GQCOR	0
MCOR	6	QCOR	896	RCOR	0	XCOR	5
XNCOR	1						
TOTAL	1063						

DETAINERS:

CDM	0	EDM	0	ENDM	0	LDM	6
MDM	0	XDM	0				
TOTAL	6						

MAINE WANTED:

CWM	0	ENM	0	EWM	0	EWMC	0
EWMJ	0	EWMJC	0	LWM	0	MWM	0
QWM	155	XNM	0	XWM	0	XWMC	0
XWMJ	0	XWMJC	0				
TOTAL	155						

PROTECTION ORDERS:

CCPO	0	CCTO	0	CENPO	0	CEPO	0
CETO	0	CMPO	43	CMTO	56	CKNPO	0
CXPO	0	CXTO	0	QWMO	19	QPOH	3
	0						
TOTAL	121						

STATE REPORTS:

ATN:

ATN	310	ATNQ	14	ATNQR	0	ATNR	0
CTN	19	CTND	5	CTNDR	0	CTNR	0
FQL	0	FQLR	0	MATN	0	MATNR	0
MCTN	4	MCTNR	0		0		
TOTAL	352						

CRIMINAL HISTORY:

FCQ	4	FCR	0	FQS	0	FRS	0
TOTAL	4						

DMV:

DQDL	0	DQPF	0	DQPI	0	DQPM	0
DQAI	0	DQCI	0	DQHA	0	DQMU	0
DQRI	0	DQTQ	29	DRCI	0	DQMR	0
DRR	0	DRPF	0	DRPM	0	DRPI	0
QVBMV	0	RQD	0				
TOTAL	29						

OTHER:

LOGOFF	1140	LOOKUP	0	LOGON	1508	XMIT	0
CHPWD	36	DSP	0	QVAD	0		0
TOTAL	2684						

Caribou PD Walk-Ins

Date	Time	Call #	Details of Walk-In
11/01/13	14:00	903	Civil
11/01/13	14:50	903	Report an accident
11/01/13	17:20	903	Complaint
11/01/13	18:01	903	Processed prisoner
11/01/13	20:54	903	Question
11/01/13	21:10	903	Subject on bath salts
11/01/13	22:25	908	Complaint
11/02/13	0:59	908	Civil
11/02/13	11:13	906	Respondants to a complaint
11/02/13	12:11	906	Paycheck
11/02/13	13:58	906	Prescription return
11/02/13	14:30	910	Dropped off Multi Handgun report
11/02/13	14:49	910	Perscription return
11/02/13	15:49	910	Lost Property
11/02/13	18:45	907	Looking to borrow ear protectors for his disabled daughter who is at CPAC, Provided
11/02/13	19:29	907	Walk in wanting to report burglary and theft young boy sat in the lobby while father spoke with officer 1/2 hour
11/03/13	3:15	913	BP Drayton came in to report suspicious activity with possible metal theft
11/03/13	5:50	912	Sharps return
11/03/13	11:28	906	Asked to assist with locked vehicle
11/03/13	11:38	906	Notorize item
11/03/13	15:10	907	Male leaving info so he can be on our road kill list
11/04/13	6:10	905	Equipment provider
11/04/13	10:30	905	Prescription return
11/04/13	11:07	915	Med return
11/04/13	11:07	915	Inspection permit
11/04/13	11:41	902	request for evidence
11/04/13	13:45	902	Fingerprint Request
11/04/13	13:00	902	Sharps return
11/04/13	14:15	910	Sharps return
11/04/13	14:21	910	Sharps return
11/04/13	16:42	910	Sharps return
11/04/13	16:42	910	Question
11/04/13	16:47	910	Sharps return

11/06/13	20:29	906	Complaint
11/06/13	21:45	909	Presque Isle, dropping off prisoner
11/07/13	8:33	906	Subject dropping items off
11/07/13	10:09	906	Inspection permit
11/07/13	13:38	906	Death certificate drop off
11/07/13	15:00	916	Dept. Homeland Security.
11/07/13	16:59	916	Kristin Leblanc in to p/up Beau Myrick's property-Jackets, hat, shoe laces, summons.
11/07/13	20:00	916	Information
11/08/13	8:00	905	subject bringing in video for officer reference assault/ Burglary
11/08/13	8:15	905	Water works indicating road closure
11/08/13	8:50	905	News requesting to speak with officer regarding Social Media
11/08/13	9:25	905	Walk in for sharps drop
11/08/13	10:00	905	Computer Crimes Unit Vassalboro to process prisoner
11/08/13	12:05	905	Female requesting assistance to obtain Protection order.
11/08/13	14:08	915	Requesting phone number for FD
11/08/13	14:27	911	Requesting to speak to officer
11/08/13	15:46	915	concealed carry
11/08/13	16:05	906	Complaint
11/08/13	22:04	908	Information about female subject to be picked up by ACSO
11/09/13	9:40	902	looking for property
11/09/13	10:15	906	complaint
11/09/13	16:20	915	Person in to see 907
11/09/13	17:40	913	Female dropping off paperwork
11/09/13	20:30	915	Female came in asking for snowmobile law book
11/09/13	21:05	915	SO transport arrived
11/09/13	23:30	913	PIPD arrived for intox (there's wasn't working)
11/10/13	0:05	913	SO arrived with prisoner, assisted in processing
11/10/13	2:35	913	BC Robertson and bailer came into bail prisoner
11/10/13	7:40	902	Burglary report for 990 Carson Rd contacted State Police
11/10/13	8:05	902	request information about titles
11/10/13	10:00	915	Sharps return
11/10/13	10:00	902	provide paper work
11/10/13	12:40	902	provide paper work
11/10/13	14:45	907	Walk in looking for gas cam. Assisted with one from the garage. Returned 10 minutes later.
11/10/13	15:18	907	Male walked in to discuss theft case with the officer.
11/10/13	16:25	907	9-1-1 call for a vehicle off the road already reported
11/10/13	16:45	907	Caller wanted to discuss criminal complaint, unable to due to cars off the road. Will call back.

11/13/13	23:50	908	Person inquiring about accidents, indicated a family member has not returned home to New Sweden
11/14/13	0:00	905	walk in for Taxi License request
11/14/13	12:15	905	Prescription return
11/14/13	12:15	905	taxi cab license request
11/15/13	8:45	902	request for permit
11/15/13	10:10	902	accident report issue
11/15/13	10:15	902	request for permit
11/15/13	15:15	903	Medication Drop Off
11/15/13	15:15	903	Medication Drop Off
11/15/13	17:19	903	Fingerprint Request
11/15/13	17:30	903	Theft complaint
11/16/13	15:22	913	Citizen dropped off unused needles to the PD for disposal
11/16/13	17:10	913	questions about deer on South Main Street
11/16/13	17:54	913	Assisted citizen in locating a plastic bag to scoop poop
11/16/13	18:22	913	Ariel Williams picked up Subpoena
11/17/13	9:22	906	Property brought in for prisoner
11/17/13	12:20	906	Interview
11/17/13	16:47	914	Individual looking for 903
11/17/13	17:00	912	Matt Cameron came in to report that there was a male in 1642RV looking through windows at his uncle funeral. Ju
11/17/13	19:43	912	Male entered the pd asking if we had his dog.
11/17/13	21:17	912	Medication return
11/18/13	11:29	907	Female asking for Off. Trainer. Will call back at 14:00
11/18/13	11:33	902	fingerprint request.
11/18/13	11:00	906	report a possible crime homicide
11/18/13	11:15	900	request for police advice.
11/18/13	14:15	914	Wellbeing check and possible bail violation(s)
11/18/13	14:30	912	Came in to fill out a statement for 907
11/18/13	15:43	912	needle drop off
11/18/13	15:58	912	needle drop off
11/18/13	22:35	909	female came in wanting information on son who was arrested this afternoon
11/19/13	8:20	907	Follow up on arrest of yesterday. Will call mother back with info on release.
11/19/13	8:45	902	request for police advice.
11/19/13	10:25	900	request for paperwork
11/19/13	11:20	900	intellegence meeting
11/19/13	12:30	902	request for information regarding unregistered car
11/19/13	12:34	902	request for BAC test
11/19/13	13:06	907	Loring Fire is back at fire house.

11/30/13	19:00	905	Squeaky walked in to get trail maps
12/01/13	20:00	913	Assisted Washburn with an uptight female prisoner

Sergeant Paul L. Vincent

From: "Stanhope, Blair" <Blair.Stanhope@maine.gov>
To: <Paul.Vincent@cariboumaine.org>
Cc: "Therault, Jackie M" <Jackie.M.Therault@maine.gov>
Sent: Friday, January 30, 2015 11:20 AM
Attach: Management Control Agreement.doc
Subject: CJIS Requirements

Paul,

Following up on our phone conversation regarding requirements for access to METRO by a non-criminal justice agency. In order for fire department personnel to access METRO for dispatch purposes for the PD, the following would need to be done:

- The area(s) utilized to access, process, and/or store METRO/CJIS data must be physically secure to prevent unauthorized personnel from having unescorted access. All points of entry need to be locked at all times.
- Anyone tasked with having direct (login) access to METRO needs to pass a fingerprint-based background check conducted by a criminal justice agency.
- Anyone having unescorted access to areas utilized to access, process, and/or store METRO/CJIS data needs to pass a fingerprint-based background check. This would include janitors/maintenance personnel and everyone with keys to these areas.
- A separate METRO Terminal Agreement would be required. This would be similar to regional communications centers which are separate entities from the law enforcement agency and not under the direct supervision of law enforcement personnel. The terminal agreement outlines responsibilities and formalizes assignment of a TAC (Terminal Agency Coordinator) and LASO (Local Agency Security Officer) for the agency connecting to METRO.
- Where the Fire Department is a non-criminal justice agency, a management control agreement (MCA) would be required. This agreement would need to stipulate that all criminal justice functions performed by the FD would be under the management control of the criminal justice agency (PD) or a board that consists of a majority of criminal justice employees. A sample MCA is attached to this email.
- Where this would need to be considered a new agency requesting METRO connectivity, an on-site visit by the ISO would need to occur to ensure physical security requirements are being met and that all parties understand roles and responsibilities associated with METRO access.
- All personnel tasked with having login access to METRO would need to complete terminal operator certification. For agencies with full access (ability to create, modify, or delete NCIC records), initial terminal operator certification entails successful completion of one-week course at the Maine Criminal Justice Academy.
- Depending on the location of the fire department in relation to the police department, work may need to be done to move the circuit and/or other network equipment used for connectivity to METRO. If such a move is needed, the Town of Caribou would be responsible for any costs incurred as a result of such move.
- The Fire Department would be subject to biennial audits for both security and quality control of all NCIC records maintained by the Caribou PD.

This list is not all-inclusive, but does give you an idea of some of the roles, responsibilities, and requirements associated with having direct access to METRO. If you or anyone else has more questions and/or concerns about the contents of this email or anything else dealing with METRO related to the changes being contemplated, please don't hesitate to contact me.

Finally, I would like to add that there are many counties and municipalities that have police dispatch for the fire

department, but this is the first time I'm aware of a municipality considering having the fire department dispatch for the police department. Again, this is not unlike how regional communications centers operate, but consideration must be made for all METRO/CJIS responsibilities and requirements that all RCC's are tasked with.

Blair

Blair Stanhope
Information Security Officer
Maine State Police
45 Commerce Drive, Suite 1
Augusta, Maine 04333
Tel. (207) 626-3920

CRIMINAL JUSTICE INFORMATION NETWORK



TERMINAL AGREEMENT – MAINE AGENCY

CRIMINAL JUSTICE INFORMATION NETWORK

TERMINAL AGENCY AGREEMENT

Pursuant to Title 25 §1508 of the Maine Revised Statutes, and subject to the conditions contained within this agreement, the Chief of the Maine State Police agrees to furnish to Caribou Police Department (hereinafter referred to as the "Terminal Agency"), a duly authorized criminal justice agency as defined in the Code of Federal Regulations (Title 28 CRF, part 20, subpart A), computer terminal access to the Criminal Justice Information Network (CJIN/METRO), for the purpose of exchanging criminal justice information.

I. Purpose of Agreement

The purpose of this document is to provide for an agreement whereby the Terminal Agency, in consideration of computer terminal access to METRO, agrees that the Maine State Police shall serve as the State Criminal Justice Information Services (CJIS) Systems Agency responsible for the regulation and quality control of the telecommunications system within the State, including, but not limited to, the exchange, dissemination and use of data contained in the Maine State Police Criminal History Record Information System, the National Crime Information Center (NCIC), a program of the Federal Bureau of Investigation's Criminal Justice Information Services Division (FBI-CJIS), the National Law Enforcement Communications System, Inc. (Nlets), the Maine State Database and other related information systems.

II. Security of Terminal

The Terminal Agency agrees to install and maintain all terminal devices in secured areas and to restrict access to such devices to only authorized personnel. The Terminal Agency further agrees to permit the Chief of the Maine State Police, the CJIS Systems Officer (CSO), or the Chief's or CSO's designee, access—at any time—to any room, building or other place where the terminal devices or related lines and circuits are located, for the purpose of inspecting the equipment and area and for any other purpose deemed appropriate or necessary by the Chief of the Maine State Police, the CSO, or the Chief's or CSO's designee, in regard to the operation of the system.

III. Security and Privacy of Data

The Terminal Agency agrees to comply with all relevant federal and Maine laws and rules and regulations adopted by the Maine State Police, FBI-CJIS, NCIC and Nlets. The Terminal Agency further agrees to protect and prohibit dissemination of information and data received from the aforementioned systems to unauthorized persons or agencies.

IV. Security of Personnel

The Terminal Agency agrees to comply with the FBI-CJIS Security Policy regarding background investigations of any person, including, but not limited to, information/technical personnel, having access to the Criminal Justice Information Network (CJIN/METRO.) At a minimum, such a background investigation must include the submission of a completed applicant fingerprint card to the State Bureau of Identification, a check of NCIC III and a check of BMV Driver License files.

V. Local Area Security Officer

The Terminal Agency agrees to comply with the FBI-CJIS Security Policy by designating one individual—identified on the last page by name and title—as the Local Area Security Officer (LASO) to act as a liaison with the Maine State Police, CJIS Systems Agency, Information Security Officer. The Terminal Agency further agrees to notify the Maine State Police within thirty (30) days of a change of LASO assignment.

See last page

VI. Maintenance Of Terminal Equipment

The Terminal Agency agrees to pay any and all costs for the installation, operation, insurance and maintenance of any required terminal equipment, which equipment shall include, but is not limited to, building modifications, terminal CRT, printer modems and supplies.

VII. Terminal Agency Coordinator

The Terminal Agency agrees to designate one individual—identified on the last page by name and title—as the Terminal Agency Coordinator (TAC) to act as liaison with the Maine State Police CJIS Systems Officer. The Terminal Agency shall submit that individual's name to the CSO of the Maine State Police upon acceptance of this agreement. The Terminal Agency further agrees to notify the Maine State Police within thirty (30) days of a change of TAC assignment.

See last page

VIII. Training of Terminal Agency Personnel

The Terminal Agency agrees to provide and pay any expenses for operating personnel to attend any required training relating to system use.

IX. Audits

The Terminal Agency agrees to permit the CJIS Systems Agency audit personnel access to all facilities housing METRO terminals for the purpose of compliance or investigative audits. The Terminal Agency further agrees to allow auditors or designated personnel access to all source documentation that supports METRO/NCIC transactions and/or entries.

X. Authority

The Chief of the Maine State Police shall have the sole discretion to promulgate any rules, regulations, policies and procedures necessary to the operation of the network.

XI. Ratification

In the event that any person who is signatory to this agreement is no longer in a position to enforce its provisions, this agreement must, within thirty (30) days, be re-entered, subject to ratification.

XII. Executory Clause

The parties hereto understand that this agreement shall be deemed executory to the extent of monies available to the Maine State Police, and no liability shall be incurred by the Maine State Police beyond monies available for that purpose.

XIII. Indemnification of the Maine State Police

In accord with the Federal Tort Claims Act, the Terminal Agency shall be liable for all claims, demands, actions, suits or proceedings founded upon the negligence or other wrongful conduct on the part of any employee of the Terminal Agency, including, but not limited to, any liability for loss or damages by reason of any claim of false arrest or false imprisonment. In no instance shall the Terminal Agency claim that the Maine State Police, or any of its agents, is so liable.

The Terminal Agency shall indemnify and hold harmless the Maine State Police, and any agents thereof, with respect to any claim, demand, action, suit or proceeding that relates to any matter governed by this agreement.

XIV. Term

The terms of this agreement shall remain in effect until the agreement is discontinued by either party. The Maine State Police reserves the right to immediately invoke the METRO Sanction policy and/or suspend furnishing any data to the Terminal Agency whenever training requirements are not met or the security, privacy, use or dissemination requirements established by federal or State law, the Maine State Police, FBI-CJIS/NCIC and/or Nlets are violated. In such instance, the Maine State Police may reinstate the furnishing of any data upon receipt of proof that the violation has been corrected. The State or Terminal Agency may, after providing a minimum thirty (30) day written notice discontinue the services contemplated by this agreement.

TERMINAL AGENCY LASO:

NAME: Michael W. Gahagan **TITLE:** Chief

TERMINAL AGENCY TAC:

NAME: Paul Vorce **TITLE:** Sgt

IN WITNESS WHEREOF, the parties hereto cause this agreement to be executed by proper officers and officials.

TERMINAL AGENCY

STATE OF MAINE
DEPARTMENT OF PUBLIC SAFETY
BUREAU OF STATE POLICE

BY: Michael W. Gahagan
PRINTED: Michael W Gahagan
TITLE: Chief
DATE: 5.24.07

BY: Jack Parkin
PRINTED: JACK PARKIN, C.S.O.
TITLE: CJIS SYSTEMS OFFICER
DATE: May 3, 2007

APPROVED:

Colonel Patrick J. Fleming

Patrick J. Fleming
CHIEF OF MAINE STATE POLICE

Requirements and Transition Document
FBI CJIS Security Policy Version 5.1
7/13/2012

Requirement Dates Between 2011-2014

Changes to the CJIS Security Policy v5.0 were approved by the Advisory Policy Board (APB) in 2011, and subsequently approved by the Director, FBI, on June 1, 2012. The policy contains current requirements carried over from version 4.5 and 5.0 along with new requirements for agencies to implement.

This document lists every new requirement and its “required by” year from 2011-2014* based on a number of factors including, among other things: cost, threat, technological innovations, and realistic need. Those cases where prior version requirements were assigned a specific “required by” date, i.e. September 30th, 2013, that date has been carried over. CJIS auditors will conduct zero-cycle audits beginning October 1st of the “required by” year. For example, new requirements with a “required by” year of 2012 will fall under the zero-cycle audit beginning October 1st, 2012. Noncriminal Justice Agencies that have not previously been subject to CJIS Security Policy audit and whose only access to FBI CJIS data is for the purpose of civil fingerprint-based background checks or other noncriminal justice purposes will not undergo zero-cycle audits until October 1st, 2013.

The “Summary of Changes” page lists requirements that were added, deleted, or changed from version 5.0 and now reflected in version 5.1. Within the transition document, these modifications are highlighted for ease of location. For continuity, there are columns on the left that reflect policy locations from version 4.5 forward. As new versions are released, these columns will change to indicate current requirement locations in the policy.

Though the dates applied to requirements are spread across several years, the intent is for agencies to start working toward them immediately, where possible, and leverage the requirements document as a tool for financial planning and justification to meet requirements that cannot be met immediately.

Please refer questions or comments about this requirements transition document or version 5.1 of the CJIS Security Policy to your respective Information Security Officer, CJIS Systems Officer, or Compact Officer.

* A requirement with “required by” year without a corresponding month and day is to be read as January 1st of that year.

SUMMARY OF CHANGES

Version 5.1

1. #20 In section 3.2.6, change the words “is to” to the word “shall”
2. #48 and #49 Split paragraph into two (2) separate requirements
3. #50 Section number changed from 4.2.2.1 to 4.2.1
4. #51 Section number changed from 4.2.2.1 to 4.2.1
5. #60 New requirement
6. #61 New requirement
7. #62 New requirement, language change from “is prohibited” to “shall not”
8. #63 New requirement, language change from “must not” to “shall not”
9. #264 Language change from “is prohibited” to “shall not”
10. #379 and #380 Split paragraph into two (2) separate requirements
11. Section 5.9.1.8 Access Records, “2. Signature of the Visitor”, requirement deleted
12. #423 New requirement
13. #431 and #432 Requirement repeated for audit purposes. Please see notes in requirements
14. #465 New requirement
15. #466 Language change in policy, added “and/or” for each sub-bullet
16. #479 New requirement
17. #486 and #487 Split paragraph into two (2) separate requirements

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
Security Policy Sections 1 - 4 (Introduction, Approach, Roles & Responsibilities, and CJ/PII)					
1	Section 2			Relationship to Local Security Policy and Other Policies	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.
2	Section 2	1.3	1.3	"	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.
3	Section 2			"	The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy.
4		New (2011) 1.3		"	The policies and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
5	Section 3.1	3.2.1		CJIS Systems Agencies (CSA)	The head of each CSA shall appoint a CJIS Systems Officer (CSO).
6		New (2011) 3.2.1	3.2.1	"	Such decisions shall be documented and kept current.
7		New (2011) 3.2.2	3.2.2	CJIS Systems Officer (CSO)	Pursuant to The Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced.
	Section 3.1 & 3.2	3.2.2		"	The CSO shall set, maintain, and enforce the following:
8	Section 3.1 & 3.2	3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJ.
9	Section 3.1 & 3.2			"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJ, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
10	Section 3.1 & 3.2	3.2.2(2)		"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
11	Section 3.1 & 3.2			"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.
12	Section 3.1 & 3.2		3.2.2(2)	"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
13		New (2011) 3.2.2(2)		"	d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
14	Section 3.1			"	e. Ensure each agency having access to CJ has someone designated as the Local Agency Security Officer (LASO).
15	Section 3.2	3.2.2(2)		"	f. Approve access to FBI CJIS systems.
16	Section 3.2			"	g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
17	Section 3.2	3.2.2(2)	3.2.2(2)	CJIS Systems Officer (CSO) (continued)	h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
		New (2011) 3.2.2(3)		"	3. Outsourcing of Criminal Justice Functions
18	Section 3.1.c	3.2.2(3)	3.2.2(3)	"	a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJJ; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJJ; and to guarantee the priority service needed by the criminal justice community.
19	Section 3.1.d			"	b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJJ; set and enforce policy governing the operation of circuits and network equipment used to transmit CJIS data; and to guarantee the priority service as determined by the criminal justice community.
20	Security Addendum Section 2.01	3.2.6	3.2.6	Contracting Government Agency (CGA)	A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an Agency Coordinator.
21	Security Addendum 2.04	3.2.7	3.2.7	Agency Coordinator (AC)	The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.
	Security Addendum 2.04	3.2.7	3.2.7	"	The AC shall :
22	Security Addendum 2.04			"	1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
23	Security Addendum 2.04			"	2. Participate in related meetings and provide input and comments for system improvement.
24	Security Addendum 2.04			"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
25	Security Addendum 2.04			"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
26	Security Addendum 2.04			"	5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
27	Security Addendum 2.04	3.2.7	3.2.7	Agency Coordinator (AC) (continued)	6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
28	Security Addendum 2.04			"	7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
29	Security Addendum 2.04			"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
30	Security Addendum 2.04			"	9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
31	Security Addendum 2.04			"	10. Any other responsibility for the AC promulgated by the FBI.
	Section 3.3	3.2.8	3.2.8	CJIS System Agency Information Security Officer (CSA ISO)	The CSA ISO shall:
32	Section 3.3			"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
33	Section 3.3			"	2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
34	Section 3.3			"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
35	Section 3.3			"	4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
	Section 3.4	3.2.9	3.2.9	Local Agency Security Officer (LASO)	Each LASO shall:
36	Section 3.4			"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
37	Section 3.4			"	2. Identify and document how the equipment is connected to the state system.
38	Section 3.4			"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.
39	Section 3.4			"	4. Ensure the approved and appropriate security measures are in place and working as expected.
40	Section 3.4	"	"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	Section 3.5	3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO shall:
41	Section 3.5			"	1. Maintain the CJIS Security Policy.
42	Section 3.5			"	2. Disseminate the FBI Director approved CJIS Security Policy.
43	Section 3.5			"	3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
44	Section 3.5			"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
45	Section 3.5			"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
46	Section 3.5			"	6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
47	Section 3.5			"	7. Maintain a current ISO homepage on the Law Enforcement Online (LEO) network and keep the CSOs and ISOs updated on pertinent information via the iso@leo.gov email address.
48		New (2011) 3.2.12	3.2.12	Compact Officer	Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer...
49		New (2011) 3.2.12		Compact Officer	...Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.
50	Section 8.2.1	4.2.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRI	The III shall be accessed only for an authorized purpose.
51	Section 8.2.1			"	Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed.
52	Section 8.2.1 & 8.2.2	4.2.1	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual.
	Section 8.2.1 & 8.2.2	4.2.1	4.2.2	"	The restricted files, which shall be protected as CHRI, are as follows:
53	Section 8.2.1 & 8.2.2			"	1. Gang File.
54	Section 8.2.1 & 8.2.2			"	2. Known or Appropriately Suspected Terrorist File.
55	Section 8.2.1 & 8.2.2			"	3. Supervised Release File.
56	Section 8.2.1 & 8.2.2			"	4. Immigration Violator File (formerly the Deported Felon File).
57	Section 8.2.1 & 8.2.2			"	5. National Sex Offender Registry File.
58	Section 8.2.1 & 8.2.2			"	6. Historical Protection Order File of the NCIC.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
59	Section 8.2.1 & 8.2.2			Proper Access, Use, and Dissemination of NCIC Restricted Files Information (continued)	7. Identity Theft File.
60			New (2012) 4.2.2	"	8. Protective Interest File.
61			New (2012) 4.2.2	"	9. Person With Information [PWI] data in the Missing Person Files.
62	Section 8.2.2.2	4.2.2.2.2	4.2.3.2	For Other Authorized Purposes	Non-restricted files information shall not be disseminated commercially.
63			New (2012) 4.2.3.2	"	Agencies shall not disseminate restricted files information for purposes other than law enforcement.
64	Section 8.6	4.2.3	4.2.4	Storage	When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.
65	Section 8.6			"	These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.
66	Section 8.3.1	4.2.4.1	4.2.5.1	Justification	In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.
67		New (2012) 4.3	4.3	Personally Identifiable Information (PII)	PII shall be extracted from CJI for the purpose of official business only.
68		New (2012) 4.3		"	Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 1 - Information Exchange Agreements					
69	Section 7.10(a) & 7.12(a) & 8.5	5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards.
70		New (2012) 5.1.1	5.1.1	Information Exchange	Before exchanging CJI, agencies shall put formal agreements in place that specify security controls.
71		New (2012) 5.1.1		Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.	
72		New (2012) 5.1.1		Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange.	
73		New (2012) 5.1.1.1	5.1.1.1	Information Handling	Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse.
74		New (2012) 5.1.1.1		Using the requirements in this policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI.	
75		Section 6.2	5.1.1.2	5.1.1.2	State and Federal Agency User Agreements
76	Section 6.2	This agreement shall include the standards and sanctions governing utilization of CJIS systems.			
77	Section 6.2	As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.			
78	New (2012) 5.1.1.2	All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.			
79	Section 6.3	5.1.1.3	5.1.1.3	Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.
80	Section 6.3			The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere.	
	Section 6.3			These agreements shall include:	
81	Section 6.3			1. Audit.	
82	Section 6.3			2. Dissemination.	
83	Section 6.3			3. Hit confirmation.	
84	Section 6.3			4. Logging.	
85	Section 6.3			5. Quality Assurance (QA).	
86	Section 6.3			6. Screening (Pre-Employment).	
87	Section 6.3			7. Security.	
88	Section 6.3			8. Timeliness.	
89	Section 6.3			9. Training.	
90	Section 6.3	10. Use of the system.			
91	Section 6.3	11. Validation.			

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
92	Section 6.4	5.1.1.4	5.1.1.4	Inter-Agency and Management Control Agreements	A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI.
93	Section 6.4			"	Access shall be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.
94	Section 6.6	5.1.1.5	5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and...
95	Section 6.6			"	...and shall be subject to the same extent of audit review as are local user agencies.
96	Security Addendum			"	All private contractors who perform criminal justice functions shall acknowledge, via signing of the Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.
97	Section 6.7			"	Modifications to the CJIS Security Addendum shall be enacted only by the FBI.
98	Section 6.6			"	1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI.
99	Section 6.6			"	Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice.
100	Section 6.6			"	The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
101	Section 6.6			"	2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI.
102	Section 6.6			"	Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice.
103	Section 6.6			"	The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
104	Section 2.1.1(b)(4)	5.1.1.6	5.1.1.6	Agency User Agreements	A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI.
105		New (2012) 5.1.1.6		"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
106	Section 2.1.1(b)(4)	5.1.1.6		"	An NCJA (public) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
107	Section 2.1.1(b)(4)	5.1.1.6	5.1.1.6	"	A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI.
108	Section 2.1.1(b)(4)	5.1.1.6		"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
109		New (2012) 5.1.1.6	5.1.1.6	Agency User Agreements (continued)	An NCJA (private) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
110	Section 2.1.1(b)(4)	5.1.1.6		"	All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance).
111		New (2012) 5.1.1.6		"	Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.
112	Section 2.1.1(b)(4)	5.1.1.7	5.1.1.7	Security and Management Control Outsourcing Standard	Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI.
113	Section 2.1.1(b)(4)	5.1.1.7		"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
114		New (2011) 5.1.1.7		"	All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard.
115	Section 6.4	5.1.1.7		"	Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.
116		New (2011) 5.1.1.7		"	Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function...
117		New (2011) 5.1.1.7		"	...and shall be subject to the same extent of audit review as are local user agencies.
118		New (2012) 5.1.2		5.1.2	Monitoring, Review, and Delivery of Services
119		New (2012) 5.1.2	"		The CJA shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response.
120		New (2012) 5.1.2	"		The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.
121		New (2012) 5.1.2.1	5.1.2.1	Managing Changes to Service Providers	Any changes to services provided by a service provider shall be managed by the CJA.
122		New (2012) 5.1.2.1		"	Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.
123		New (2012) 5.1.3	5.1.3	Secondary Dissemination	If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 2 - Security Awareness Training					
124		New (2013) 5.2	5.2	Policy Area 2: Security Awareness Training	Basic security awareness training shall be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJI.
125		New (2013) 5.2.1.1	5.2.1.1	All Personnel	At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:
126				"	1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
127				"	2. Implications of noncompliance.
128				"	3. Incident response (Points of contact; Individual actions).
129				"	4. Media Protection.
130				"	5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
131				"	6. Protect information subject to confidentiality concerns — hardcopy through destruction.
132				"	7. Proper handling and marking of CJI.
133				"	8. Threats, vulnerabilities, and risks associated with handling of CJI.
134				New (2013) 5.2.1.2	5.2.1.2
135		"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.		
136		"	2. Password usage and management—including creation, frequency of changes, and protection.		
137		"	3. Protection from viruses, worms, Trojan horses, and other malicious code.		
138		"	4. Unknown e-mail/attachments.		
139		"	5. Web usage—allowed versus prohibited; monitoring of user activity.		
140		"	6. Spam.		
141		"	7. Social engineering. (The act of manipulating people to perform actions or divulging confidential information.)		
142		"	8. Physical Security—increases in risks to systems and data.		
143		"	9. Media Protection.		
144		"	10. Handheld device security issues—address both physical and wireless security issues.		
145		"	11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.		
146		"	12. Laptop security—address both physical and information security issues.		
147		"	13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).		
148		"	14. Access control issues—address least privilege and separation of duties.		
				"	15. Individual accountability—explain what this means in the agency.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement	
149		New (2013) 5.2.1.2	5.2.1.2	Personnel with Physical and Logical Access (continued)	16. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.	
150				"	17. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems.	
151				"	18. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.	
152				"	19. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.	
153		New (2013) 5.2.1.3	5.2.1.3	Personnel with Information Technology Roles	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):	
154				"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.	
155				"	2. Data backup and storage—centralized or decentralized approach.	
156				"	3. Timely application of system patches—part of configuration management.	
157				"	4. Access control measures.	
158		Section 4.3	5.2.2	5.2.2	Security Training Records	Records of individual basic security awareness training and specific information system security training shall be:
159						- documented
160			- kept current			
161	New (2013) 5.2.2		- maintained by the CSO/SIB/Compact Officer			

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 3 - Incident Response					
162		New (2012) 5.3	5.3	Policy Area 3: Incident Response	Agencies shall : (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.
163		New (2012) 5.3		"	ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.
164		New (2012) 5.3.1	5.3.1	Reporting Information Security Events	The agency shall promptly report incident information to appropriate authorities.
165		New (2012) 5.3.1		"	Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.
166	Sections 3.3(d) & 5.2.2	5.3.1		"	Formal event reporting and escalation procedures shall be in place.
167		New (2012) 5.3.1		"	Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents.
168		New (2012) 5.3.1		"	All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.
	Section 5.2.1	5.3.1.1.1	5.3.1.1.1	FBI CJIS Division Responsibilities	The FBI CJIS Division shall :
169	Section 5.2.1			"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
170	Section 5.2.1			"	2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
171	Section 5.2.1			"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
172	Section 5.2.1			"	4. Disseminate prompt advisories of system threats and operating system vulnerabilities to all CSOs and ISOs through the use of the iso@leo.gov e-mail account, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
173	Section 5.2.1			"	5. Track all reported incidents and/or trends.
174	Section 5.2.1			"	6. Monitor the resolution of all incidents.
	Section 5.5.2	5.3.1.1.2	5.3.1.1.2	CSA ISO Responsibilities	The CSA ISO shall :
175	Section 5.5.2			"	1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
176	Section 5.5.2			"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
177	Section 5.5.2			"	3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
178	Section 5.5.2	5.3.1.1.2	5.3.1.1.2	CSA ISO Responsibilities (continued)	4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
179	Section 5.5.2			"	5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
180	Section 5.5.2			"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.
181		New (2012) 5.3.2	5.3.2	Management of Information Security Incidents	A consistent and effective approach shall be applied to the management of information security incidents.
182	Section 5.3 & 5.4	5.3.2		"	Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.
183		New (2012) 5.3.2.1	5.3.2.1	Incident Handling	The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
184		New (2013) 5.3.2.1		"	Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.
185		New (2012) 5.3.2.2	5.3.2.2	Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
186		New (2012) 5.3.3	5.3.3	Incident Response Training	The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.
187		New (2012) 5.3.4	5.3.4	Incident Monitoring	The agency shall track and document information system security incidents on an ongoing basis.
188		New (2012) 5.3.4		"	The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete (whichever time-frame is greater).

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 4 - Auditing and Accountability					
189		New (2013) 5.4	5.4	Policy Area 4: Auditing and Accountability	Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.
190		New (2013) 5.4		"	Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.
191	Section 7.14	5.4.1	5.4.1	Auditable Events and Content (Information Systems)	The agency's information system shall generate audit records for defined events.
192		New (2013) 5.4.1		"	The agency shall specify which information system components carry out auditing activities.
193	Section 7.14	5.4.1		"	The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
194		New (2013) 5.4.1		"	The agency shall periodically review and update the list of agency-defined auditable events.
195		New (2013) 5.4.1		"	In the event an agency does not use an automated system, manual recording of activities shall still take place.
	Section 7.14	5.4.1.1		5.4.1.1	Events
196	Section 7.14	5.4.1.1	"		1. Successful and unsuccessful system log-on attempts.
197		New (2013) 5.4.1.1	"		2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
198	Section 7.14	5.4.1.1	"		3. Successful and unsuccessful attempts to change account passwords.
199		New (2013) 5.4.1.1	"		4. Successful and unsuccessful actions by privileged accounts.
200			"		5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
201			New (2013) 5.4.1.1.1		Content
202		5.4.1.1.1		"	1. Date and time of the event.
203		"		"	2. The component of the information system (e.g., software component, hardware component) where the event occurred.
204		"		"	3. Type of event.
205		"		"	4. User/subject identity.
206		New (2013) 5.4.2	5.4.2	Response to Audit Processing Failures	The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure.
207		New (2013) 5.4.3	5.4.3	Audit Monitoring, Analysis, and Reporting	The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.
208		New (2013) 5.4.3		"	Audit review/analysis shall be conducted at a minimum once a week.
209		New (2013) 5.4.3		"	The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
210		New (2013) 5.4.4	5.4.4	Time Stamps	The agency's information system shall provide time stamps for use in audit record generation.
211		New (2013) 5.4.4		"	The time stamps shall include the date and time values generated by the internal system clocks in the audit records.
212	Section 7.14	5.4.4		"	The agency shall synchronize internal information system clocks on an annual basis.
213		New (2013) 5.4.5	5.4.5	Protection of Audit Information	The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.
214		New (2012) 5.4.6	5.4.6	Audit Record Retention	The agency shall retain audit records for at least 365 days.
215		New (2013) 5.4.6		"	Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.
216	Section 8.4	5.4.7	5.4.7	Logging NCIC and III Transactions	A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions.
217	Section 8.4	5.4.7		"	The III portion of the log shall clearly identify both the operator and the authorized receiving agency.
218	Section 8.4	5.4.7		"	III logs shall also clearly identify the requester and the secondary recipient.
219	Section 8.4	5.4.7		"	The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement	
CJIS Security Policy Area 5 - Access Control						
220		New (2012) 5.5.1	5.5.1	Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	
221		New (2012) 5.5.1		"	The agency shall validate information system accounts at least annually and...	
222		New (2012) 5.5.1		"	...and shall document the validation process.	
223		New (2013) 5.5.1		"	The agency shall identify authorized users of the information system and specify access rights/privileges.	
224		New (2013) 5.5.1		"	The agency shall grant access to the information system based on:	
225				"	1. Valid need-to-know/need-to-share that is determined by assigned official duties.	
226		New (2013) 5.5.1		"	2. Satisfaction of all personnel security criteria.	
227				"	The agency responsible for account creation shall be notified when:	
228	Section 7.6	5.5.2			Access Enforcement	1. A user's information system usage or need-to-know or need-to-share changes.
229		New (2012) 5.5.2		5.5.2	"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.
230		New (2013) 5.5.2	"		The information system shall enforce assigned authorizations for controlling access to the system and contained information.	
231		New (2013) 5.5.2.1	5.5.2.1	Least Privilege	The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.	
232		New (2013) 5.5.2.1		"	Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.	
233	Section 7.6.3	5.5.2.1		"	The agency shall approve individual access privileges and...	
234		New (2013) 5.5.2.1		"	...and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes.	
235		New (2013) 5.5.2.2	5.5.2.2	System Access Control	The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.	
236		New (2013) 5.5.2.2		"	Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.	
					Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.	
					Access controls shall be in place and operational for all IT systems to:	

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
237		New (2013) 5.5.2.2	5.5.2.2	System Access Control (continued)	1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
238		New (2013) 5.5.2.2	5.5.2.2	"	2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.
239		New (2013) 5.5.2.3	5.5.2.3	Access Control Criteria	Agencies shall control access to CJI based on one or more of the following:
240				"	1. Job assignment or function (i.e., the role) of the user seeking access.
241				"	2. Physical location.
242				"	3. Logical location.
243				"	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
				"	5. Time-of-day and day-of-week/month restrictions.
		New (2013) 5.5.2.4	5.5.2.4	Access Control Mechanisms	When setting up access controls, agencies shall use one or more of the following mechanisms:
244				"	1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
245				"	2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
246				"	3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.1.2 for encryption requirements).
247				"	4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.
248	Section 7.6.1	5.5.3	5.5.3	Unsuccessful Login Attempts	Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI).
249	Section 7.6.1	5.5.3		"	The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.
250		New (2013) 5.5.4	5.5.4	System Use Notification	The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.
		New (2013) 5.5.4	5.5.4	"	The system use notification message shall , at a minimum, provide the following information:
251				"	1. The user is accessing a restricted information system.
252				"	2. System usage may be monitored, recorded, and subject to audit.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
253		New (2013) 5.5.4	5.5.4	System Use Notification (continued)	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
254				"	4. Use of the system indicates consent to monitoring and recording.
255		New (2013) 5.5.4	5.5.4	"	The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.
256				New (2013) 5.5.4	"
257	Section 7.6.2, Change 1	5.5.5	5.5.5	Session Lock	The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
258		New (2013) 5.5.5		"	Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.
259		New (2013) 5.5.6	5.5.6	Remote Access	The agency shall authorize, monitor, and control all methods of remote access to the information system.
260		New (2013) 5.5.6		"	The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.
261		New (2013) 5.5.6		"	The agency shall control all remote accesses through managed access control points.
262		New (2013) 5.5.6		"	The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.
263		New (2011) 5.5.6.1		5.5.6.1	Personally Owned Information Systems
264		New (2012) 5.5.6.2	5.5.6.2	Publicly Accessible Computers	Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
265		New (2012) 5.5.7	5.5.7	Wireless Access Restrictions	The agency shall :
266	"			(i) establish usage restrictions and implementation guidance for wireless technologies;	
			"	(ii) authorize, monitor, control wireless access to the information system.	
267	New (2012) 5.5.7.1	5.5.7.1	All 802.11x Wireless Protocols	Agencies shall :	
268			"	1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.	
269			"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	
			"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
270		New (2012) 5.5.7.1	5.5.7.1	All 802.11x Wireless Protocols (continued)	4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
271		New (2012) 5.5.7.1	5.5.7.1	"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.
272				"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.
273				"	7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
274				"	8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
275				"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
276				"	10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
277				"	11. Ensure that the ad hoc mode has been disabled unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
278				"	12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
279				"	13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
280				"	14. Segregate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
281				"	15. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
		New (2012) 5.5.7.2	5.5.7.2	Legacy 802.11 Protocols	Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.
282				"	1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
283				"	2. Enable WEP/WPA.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
284		New (2012) 5.5.7.2	5.5.7.2	Legacy 802.11 Protocols (continued)	3. Ensure the default shared keys are replaced by more secure unique keys.
285				"	4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.
286		New (2012) 5.5.7.3.1	5.5.7.3.1	Cellular Risk Mitigations	Organizations shall , as a minimum, ensure that cellular devices:
287				"	1. Apply available critical patches and upgrades to the operating system.
288				"	2. Are configured for local device authentication.
289				"	3. Use advanced authentication.
290				"	4. Encrypt all CJI resident on the device.
291				"	5. Erase cached information when session is terminated.
292				"	6. Employ personal firewalls.
293		New (2012) 5.5.7.4	5.5.7.4	Bluetooth	If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.
294		New (2012) 5.5.7.4	5.5.7.4	"	Agencies shall :
295				"	1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
296				"	2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
297				"	3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy.
298				"	4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).
				"	5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN shall be used.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
299		New (2012) 5.5.7.4	5.5.7.4	Bluetooth (continued)	6. For v2.1 devices using Secure Simple Pairing, avoid using the "Just Works" model. The "Just Works" model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
300		New (2012) 5.5.7.4	5.5.7.4	"	7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
301	"			8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.	
302	"			9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.	
303	"			10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.	
304	"			11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.	
305	"			12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.	
306	"			13. Establish a "minimum key size" for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.1.2 for minimum key encryption standards.	
307	"			14. Use Security Mode 3 in order to provide link-level security prior to link establishment.	
308	"			15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.	

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 6 - Identification and Authentication					
309		New (2012) 5.6	5.6	Policy Area 6: Identification and Authentication	The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.
310	Section 7.3.1	5.6.1	5.6.1	Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified.
311	Section 7.3.1	5.6.1		"	A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit.
312	Section 7.3.1	5.6.1		"	Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system.
313	Section 7.3.1	5.6.1		"	Agencies shall ensure that all user IDs belong to currently authorized users.
314	Section 7.3.1	5.6.1		"	Identification data shall be kept current by adding new users and disabling and/or deleting former users.
315	Section 6.1	5.6.1.1	5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction.
316	Section 6.1	5.6.1.1		"	The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.
317	Section 6.1	5.6.1.1		"	Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.
318	Section 6.1	5.6.1.1		"	Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.
319		New (2011) 5.6.2	5.6.2	Authentication Policy and Procedures	Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level.
320	Section 7.3.2.2	5.6.2		"	The authentication strategy shall be part of the agency's audit for policy compliance.
321	Section 7.3.2.2	5.6.2		"	The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services.
322		New (2011) 5.6.2		"	The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.
323	Section 7.3.3	5.6.2.1	5.6.2.1	Standard Authentication (Password)	Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID.
	Section 7.3.3	5.6.2.1		"	Passwords shall :
324	Section 7.3.3			"	1. Be a minimum length of eight (8) characters on all systems.
325	Section 7.3.3			"	2. Not be a dictionary word or proper name.
326	Section 7.3.3			"	3. Not be the same as the Userid.
327	Section 7.3.3		"	4. Expire within a maximum of 90 calendar days.	

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement		
328	Section 7.3.3	5.6.2.1	5.6.2.1	Standard Authentication (Password) (continued)	5. Not be identical to the previous ten (10) passwords.		
329	Section 7.3.3			"	6. Not be transmitted in the clear outside the secure location.		
330		New (2012) 5.6.2.1	5.6.2.2.1	"	7. Not be displayed when entered.		
331		New (2012) 5.6.2.2.1		"	EXCEPTION: AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access.		
332	Section 7.3.2.2	5.6.3	5.6.3	Identifier and Authenticator Management	The agency shall establish identifier and authenticator management processes.		
333		New (2012) 5.6.3.1	5.6.3.1	Identifier Management	The agency shall document and manage user identifiers by:		
334				"	1. Uniquely identifying each user.		
335				"	2. Verifying the identity of each user.		
336				"	3. Receiving authorization to issue a user identifier from an appropriate agency official.		
337				"	4. Issuing the user identifier to the intended party.		
338				"	5. Disabling the user identifier after a specified period of inactivity.		
339				"	6. Archiving user identifiers.		
340				New (2012) 5.6.3.2	5.6.3.2	Authenticator Management	In order to manage information system authenticators, agencies shall :
341						"	1. Define initial authenticator content.
342						"	2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
343	"	3. Change default authenticators upon information system installation.					
344	New (2014) 5.6.4	5.6.4	Assertions	Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.			
345			"	Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:			
346			"	1. Digitally signed by a trusted entity (e.g., the identity provider).			
347			"	2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.			
		New (2014) 5.6.4		"	Assertions generated by a verifier shall expire after 12 hours and...		
		New (2014) 5.6.4		"	...and shall not be accepted thereafter by the relying party.		

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 7 - Configuration Management					
348		New (2011) 5.7.1.1	5.7.1.1	Least Functionality	The agency shall configure the application, service, or information system to provide only essential capabilities and...
349		New (2011) 5.7.1.1		Least Functionality	...and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
350	Section 7.1	5.7.1.2	5.7.1.2	Network Diagram	The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.
	Section 7.1	5.7.1.2		"	The network topological drawing shall include the following:
351	Section 7.1			"	1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
352	Section 7.1			"	2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
353	Section 7.1			"	3. "For Official Use Only" (FOUO) markings.
354				New (2012) 5.7.1.2	"
355		New (2012) 5.7.2	5.7.2	Security of Configuration Documentation	Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 8 - Media Protection					
356		New (2011) 5.8	5.8	Policy Area 8: Media Protection	Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.
357		New (2011) 5.8		"	Procedures shall be defined for securely handling, transporting and storing media.
358		New (2011) 5.8.1	5.8.1	Media Storage and Access	The agency shall securely store electronic and physical media within physically secure locations or controlled areas.
359		New (2011) 5.8.1		"	The agency shall restrict access to electronic and physical media to authorized individuals.
360		New (2013) 5.8.1		"	If physical and personnel restrictions are not feasible then the data shall be encrypted per section 5.10.1.2.
361		New (2011) 5.8.2	5.8.2	Media Transport	The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
362		New (2011) 5.8.2.1	5.8.2.1	Electronic Media in Transit	Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.
363		New (2011) 5.8.2.1		"	Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute other controls to ensure the security of the data.
364		New (2011) 5.8.2.2	5.8.2.2	Physical Media in Transit	Physical media shall be protected at the same level as the information would be protected in electronic form.
365	Section 4.6 & 4.7	5.8.3	5.8.3	Electronic Media Sanitization and Disposal	The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.
366	Section 4.6(a)	5.8.3		"	Inoperable electronic media shall be destroyed (cut up, shredded, etc.).
367	Section 4.7	5.8.3		"	The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media.
368		New (2011) 5.8.3		"	Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
369		New (2011) 5.8.4	5.8.4	Disposal of Physical Media	Physical media shall be securely disposed of when no longer required, using formal procedures.
370		New (2011) 5.8.4		"	Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals.
371	Section 4.6	5.8.4		"	Physical media shall be destroyed by shredding or incineration.
372		New (2011) 5.8.4		"	Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 9 - Physical Protection					
373		New (2011) 5.9	5.9	Policy Area 9: Physical Protection	Physical protection policy and procedures shall be documented and implemented to ensure CJ and information system hardware, software, and media are physically protected through access control measures.
374		New (2011) 5.9.1	5.9.1	Physically Secure Location	For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30 th 2013.
375	Section 7.2.2	5.9.1.1	5.9.1.1	Security Perimeter	The perimeter of physically secure location shall be prominently posted and separated from non-secure locations by physical controls.
376	Section 7.2.2	5.9.1.1		"	Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.
377		New (2013) 5.9.1.2	5.9.1.2	Physical Access Authorizations	The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or...
378		New (2013) 5.9.1.2	5.9.1.2	Physical Access Authorizations	...or shall issue credentials to authorized personnel.
379	Section 4.4.1	5.9.1.3	5.9.1.3	Physical Access Control	The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and...
380		New (2011) 5.9.1.3		"	...and shall verify individual access authorizations before granting access.
381	Section 4.4.1	5.9.1.4	5.9.1.4	Access Control for Transmission Medium	The agency shall control physical access to information system distribution and transmission lines within the physically secure location.
382	Section 4.4.1	5.9.1.5	5.9.1.5	Access Control for Display Medium	The agency shall control physical access to information system devices that display CJ and...
383	Section 4.4.1	5.9.1.5		Access Control for Display Medium	...and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJ.
384	Section 4.4.1	5.9.1.6	5.9.1.6	Monitoring Physical Access	The agency shall monitor physical access to the information system to detect and respond to physical security incidents.
385	Section 4.4.1	New (2011) 5.9.1.7	5.9.1.7	Visitor Control	The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).
386	Section 4.4.3	New (2011) 5.9.1.7		"	The agency shall escort visitors at all times and monitor visitor activity.
387		New (2012) 5.9.1.8	5.9.1.8	Access Records	The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publicly accessible) that includes:
388				"	1. Name and agency of the visitor.
389			"	2. Signature of the visitor. NOTE: REMOVED FROM POLICY	
390			"	3. Form of identification.	
391			"	4. Date of access.	
392			"	5. Time of entry and departure.	
393			"	6. Purpose of visit.	
394			"	7. Name and agency of person visited.	
					The visitor access records shall be maintained for a minimum of one year.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
395		New (2012) 5.9.1.8	5.9.1.8	Access Records (continued)	Designated officials within the agency shall frequently review the visitor access records for accuracy and completeness.
396		New (2013) 5.9.1.9	5.9.1.9	Delivery and Removal	The agency shall authorize and control information system-related items entering and exiting the physically secure location .
397		New (2013) 5.9.2	5.9.2	Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a "controlled area" for the purpose of day-to-day CJI access or storage.
398		New (2012) 5.9.2		"	The agency shall , at a minimum:
399				"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
400				"	2. Lock the area, room, or storage container when unattended.
401				"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
			"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.	

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity					
402	Section 7.5	5.10.1	5.10.1	Information Flow Enforcement	The network infrastructure shall control the flow of information between interconnected systems.
		New (2013) 5.10.1.1	5.10.1.1	Boundary Protection	The agency shall :
403	Section 7	5.10.1.1		"	1. Control access to networks processing CJI.
404		New (2013) 5.10.1.1		"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
405	Section 7.5 & 7.13	5.10.1.1		"	3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.
406		New (2013) 5.10.1.1		"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
407		New (2011) 5.10.1.1		"	5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").
408		New (2012) 5.10.1.1		"	6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in section 5.10.3.2 to achieve separation.
409	Section 7.9 & 7.12	5.10.1.2	5.10.1.2	Encryption	1. Encryption shall be a minimum of 128 bit.
410	Section 7.9	5.10.1.2		"	2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).
411		New (2013) 5.10.1.2		"	3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
412	Section 7.9 & 7.12	5.10.1.2		"	4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
413		New (2013) 5.10.1.2		"	5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.
414		New (2013) 5.10.1.2		"	Registration to receive a public key certificate shall :
415				"	a) Include authorization by a supervisor or a responsible official.
416				"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.
417		New (2013) 5.10.1.3	5.10.1.3	Intrusion Detection Tools and Techniques	The agency shall implement network-based and/or host-based intrusion detection tools.
		New (2012) 5.10.1.3		"	The CSA/SIB shall , in addition:
418				"	1. Monitor inbound and outbound communications for unusual or unauthorized activities.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement	
419		New (2012) 5.10.1.3	5.10.1.3	Intrusion Detection Tools and Techniques (continued)	2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.	
420				"	3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	
421		New (2011) 5.10.1.4	5.10.1.4	Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:	
422				"	1. Establish usage restrictions and implementation guidance for VoIP technologies.	
423				"	2. Document, monitor and control the use of VoIP within the agency.	
424			New (2012) 5.10.3.1	5.10.3.1	Partitioning	The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.
425					New (2012) 5.10.3.1	"
426			New (2012) 5.10.3.2	5.10.3.2	Virtualization	In addition to the security controls described in this policy, the following additional controls shall be implemented in a virtual environment:
427					"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
428					"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
429					"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally.
430			New (2011) 5.10.4.1	5.10.4.1	Patch Management	The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
431					Section 7.13.1(d)	Patch Management
432					New (2011) 5.10.4.1	Patch Management

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
433		New (2012) 5.10.4.1	5.10.4.1	Patch Management (continued)	Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.
434		New (2012) 5.10.4.2	5.10.4.2	Malicious Code Protection	The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access.
435		New (2012) 5.10.4.2		"	Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).
436	Section 7.15	5.10.4.2		"	The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network.
437		New (2011) 5.10.4.2		"	The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
438		New (2012) 5.10.4.3		5.10.4.3	Spam and Spyware Protection
439		New (2012) 5.10.4.3	"		The agency shall :
440			"		1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
441			"		2. Employ spyware protection at workstations, servers or mobile computing devices on the network.
			"		3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this policy document.
442	Section 7.13.3		5.10.4.4	5.10.4.4	Personal Firewall
	Section 7.13.3(b)	5.10.4.4	"		At a minimum, the personal firewall shall perform the following activities:
443	Section 7.13.3(b)		"		1. Manage program access to the Internet.
444	Section 7.13.3(b)		"		2. Block unsolicited requests to connect to the PC.
445	Section 7.13.3(b)		"		3. Filter Incoming traffic by IP address or protocol.
446	Section 7.13.3(b)		"		4. Filter Incoming traffic by destination ports.
447	Section 7.13.3(b)		"		5. Maintain an IP traffic log.
448			New (2012) 5.10.4.5	5.10.4.5	Security Alerts and Advisories
449		"			1. Receive information system security alerts/advisories on a regular basis.
450		"			2. Issue alerts/advisories to appropriate personnel.
451		"			3. Document the types of actions to be taken in response to security alerts/advisories.
452		"			4. Take appropriate actions in response.
				5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	
453	Section 7.6	5.10.4.6	5.10.4.6	Information Input Restrictions	The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 11 - Formal Audits					
454	Section 9.2	5.11.1.1	5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.
455	Section 9.2	5.11.1.1		"	This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs.
456		New (2013) 5.11.1.1		"	The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
457		New (2013) 5.11.1.2	5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit shall include a sample of CJAs and NCJAs.
	Section 9.1		5.11.2	Audits by the CSA	Each CSA shall :
458	Section 9.1	5.11.2		"	1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
459		New (2013) 5.11.2		"	2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
460				"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
461	Section 9.4	5.11.3		5.11.3	Special Security Inquiries and Audits
462	Section 9.4	5.11.3	"		The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division.
463	Section 9.4	5.11.3	"		All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
CJIS Security Policy Area 12 - Personnel Security					
464	Section 4.5.1(a)	5.12.1.1	5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI	1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
465			New (2013) 5.12.1.1	"	However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
466		New (2012) 5.12.1.1	5.12.1.1	"	When appropriate, the screening shall be consistent with (i) 5 CFR 731.106; and/or (ii) Office of Personnel Management policy, regulations, and guidance; and/or (iii) agency policy, regulations, and guidance.
467	Section 4.5.1(a)	5.12.1.1	5.12.1.1	"	2. All requests for access shall be made as specified by the CSO.
468	Section 4.5.1(a)	5.12.1.1		"	All CSO designees shall be from an authorized criminal justice agency.
469	Section 4.5.1(b)	5.12.1.1		"	3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI.
470	Section 4.5.1(c)	5.12.1.1		"	4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
471	Section 4.5.1(d)	5.12.1.1		"	5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
472	Section 4.5.1(e)	5.12.1.1		"	6. If the person is employed by a noncriminal justice agency, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate.
473		New (2011) 5.12.1.1		"	7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO.
474	Section 4.5.1(g)	5.12.1.1		"	8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
475	Section 4.5.1(g)	5.12.1.1		"	8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
476	Section 4.5.1(h)	5.12.1.1		"	9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
477	Security Addendum 6.00	5.12.1.2	5.12.1.2	Personnel Screening for Contractors and Vendors	In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:
478	Security Addendum 6.03	5.12.1.2	5.12.1.2	"	1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record checks.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
479			New (2013) 5.12.1.2	Personnel Screening for Contractors and Vendors (continued)	However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
480	Security Addendum 6.03(b)	5.12.1.2	5.12.1.2	"	2. If a record of any kind is found, the CGA shall be formally notified, and...
481	Security Addendum 6.03(b)	5.12.1.2		"	...and system access shall be delayed pending review of the criminal history record information.
482	Security Addendum 6.03(b)	5.12.1.2		"	The CGA shall in turn notify the Contractor-appointed Security Officer.
483	Security Addendum 6.03(c)	5.12.1.2		"	3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
484		New (2012) 5.12.1.2		"	4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
485		New (2012) 5.12.1.2		"	5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
486		New (2012) 5.12.1.2		5.12.1.2	"
487		New (2012) 5.12.1.2	"		6.and shall , upon request, provide a current copy of the access list to the CSO.
488		New (2012) 5.12.3	5.12.3	Personnel Transfer	The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.
489	Section 4.2	5.12.4	5.12.4	Personnel Sanctions	The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.



Aroostook Technologies, Inc.

(207) 764-1463 Fax
 4 Airport Dr.
 Presque Isle, ME 04769

Proposal

Bill To:	Ship To:
Caribou Police Dept. 25 High St. Caribou, Maine 04736	Caribou Police Dept. 25 High St. Caribou, Maine 04736

Rep.	Proposal Date	Job Type	Terms	Job Name	Proposal No.
KGD	2/9/2015		Net 15		30422

Qty	Part No.	Description	Price	Total
1	Installation Labor	Installation / Removal Labor Chief Gahagan, This is only a Budgetary proposal for moving the Police department radio equipment to the Fire department. We would recommend that a tower be installed on the building, this is because of the multiple radios and antennas. We would need to do a walk through of both departments with you and Chief Susi to get a full scope of the project to be able give you a accurate proposal of what is needed to do this project. If you have any questions on this budgetary proposal, please feel free to call us. Thank you, Kenny Dufour	15,000.00	15,000.00

Customer Signature: _____ Date: _____ Salesman Signature: _____ Date: _____	Subtotal	\$15,000.00
	Sales Tax (0.0%)	\$0.00
	Total	\$15,000.00

This proposal is valid for 60 days. Each manufacturer of products sold by Aroostook Technologies Inc. (ATI) provides warranties for it's products and sets procedures for processing their warranty claims. Defective products may require returning them to the manufacturer for repair or replacement. ATI warrants it's installations to be free from defects for 90 days. Any shipping, travel, mileage or other costs incurred by ATI in the handling of factory warrantied products will be billed to the product owner unless the manufacturer has a warranty reimbursement program. ATI shall not be responsible for any incidental or consequential damages sustained by the purchaser by burglary, theft, fire, misuse, personal injury or any other cause that may arise due to a defect in the system or product.

<i>Androscoggin County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Androscoggin SO	—	—	—	3	4	2	84	137	8	—	238	28.6
Auburn	22,948	48.37	—	6	10	20	197	858	17	2	1,110	45.6
Lewiston	36,422	36.76	—	19	20	62	313	848	56	21	1,339	21.9
Livermore Falls	3,161	28.47	—	—	—	2	15	71	2	—	90	23.3
Lisbon	8,923	11.77	—	3	1	3	14	80	4	—	105	44.8
Mechanic Falls	3,013	12.61	—	1	—	5	11	19	1	1	38	55.3
Sabattus	5,060	17.00	—	3	—	3	33	44	3	—	86	51.2
Androscoggin SP	—	—	1	1	1	3	36	65	8	3	118	29.7
Androscoggin County Totals	107,469	29.07	1	36	36	100	703	2,122	99	27	3,124	33.1
Total Urban Areas	79,527	34.81	—	32	31	95	583	1,920	83	24	2,768	33.7
Total Rural Areas	27,942	12.74	1	4	5	5	120	202	16	3	356	28.9

<i>Aroostook County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Aroostook SO	—	—	—	—	—	—	23	44	5	—	72	16.7
Caribou	8,012	14.73	—	—	1	5	26	80	6	—	118	72.0
Fort Fairfield	3,412	15.24	—	—	—	4	8	38	2	—	52	90.4
Fort Kent	4,055	3.45	—	—	—	2	—	11	1	—	14	71.4
Houlton	6,046	24.64	—	2	—	4	27	115	1	—	149	56.4
Madawaska	3,957	9.60	—	1	—	1	3	32	1	—	38	52.6
Presque Isle	9,483	18.35	—	4	1	8	9	150	2	—	174	60.3
Van Buren	2,125	7.06	—	—	—	—	6	7	2	—	15	73.3
Ashland	1,277	9.40	—	—	—	—	7	4	1	—	12	25.0
Limestone	2,269	9.70	—	—	—	3	5	9	2	3	22	22.7
Washburn	1,651	22.41	—	—	—	1	8	27	1	—	37	16.2
Aroostook SP	—	—	4	—	—	8	125	136	7	4	284	40.1
Aroostook County Totals	70,507	14.00	4	7	2	36	247	653	31	7	987	50.9
Total Urban Areas	42,287	14.92	—	7	2	28	99	473	19	3	631	59.6
Total Rural Areas	28,220	12.62	4	—	—	8	148	180	12	4	356	35.4

<i>Cumberland County</i>			<i>January–December 2013</i>									
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Cumberland SO	—	—	—	3	4	24	266	439	32	5	773	29.0
Brunswick	20,354	26.14	—	8	4	11	90	409	10	—	532	33.7
Cape Elizabeth	9,104	10.98	—	—	—	—	26	70	2	2	100	30.0
Falmouth	11,468	11.77	1	1	1	2	19	106	3	2	135	62.2
Gorham	16,764	10.80	—	2	1	11	36	121	7	3	181	34.3
Portland	66,256	42.18	1	21	85	70	383	2,160	69	6	2,795	23.0
South Portland	25,126	36.73	—	5	13	44	113	722	26	—	923	32.2
Scarborough	19,252	22.75	—	7	2	9	66	343	11	—	438	32.9
Westbrook	17,647	35.25	1	11	6	20	78	485	20	1	622	43.1
Bridgton	5,308	7.54	—	1	1	5	6	25	2	—	40	55.0
Cumberland	7,353	2.72	—	—	—	1	11	7	1	—	20	30.0
Freeport	8,094	19.89	1	—	—	2	25	129	4	—	161	37.3
Yarmouth	8,460	9.34	—	2	1	3	19	52	1	1	79	25.3
Windham	17,363	18.66	—	—	2	7	53	248	12	2	324	34.6
University of Southern Maine	—	—	—	—	—	—	7	35	—	—	42	4.8
Cumberland MDEA	—	—	—	—	—	—	—	1	—	—	1	100.0
Cumberland SP	—	—	1	—	—	3	14	24	5	—	47	31.9
Cumberland County Totals	284,432	25.36	5	61	120	212	1,212	5,376	205	22	7,213	30.1
Total Urban Areas	232,549	27.49	4	58	116	185	932	4,913	168	17	6,393	30.2
Total Rural Areas	51,883	15.80	1	3	4	27	280	463	37	5	820	29.1

<i>Franklin County</i>			<i>January–December 2013</i>									
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Franklin SO	—	—	—	5	2	7	22	47	4	—	87	20.7
Farmington	7,657	28.99	—	1	—	11	23	184	3	—	222	32.4
Jay	4,827	24.24	—	1	1	1	30	80	3	1	117	18.0
Wilton	4,066	12.05	—	—	—	5	16	28	1	—	49	34.7
Rangeley	1,176	24.66	—	—	—	1	10	17	1	—	29	10.3
University of ME Farmington	—	—	—	—	—	—	2	15	—	—	17	11.8
Carrabassett Valley	780	67.95	—	—	—	—	4	49	—	—	53	3.8
Franklin SP	—	—	—	—	—	6	32	37	2	—	77	37.7
Franklin County Totals	30,568	21.30	—	6	3	31	139	457	14	1	651	25.2
Total Urban Areas	18,506	26.32	—	1	1	18	85	373	8	1	487	24.0
Total Rural Areas	12,062	13.60	—	5	2	13	54	84	6	—	164	28.7

<i>Hancock County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Hancock SO	—	—	—	—	1	3	49	129	7	—	189	35.4
Bar Harbor	5,275	15.36	—	—	2	1	19	59	—	—	81	28.4
Ellsworth	7,853	35.53	1	—	1	3	57	209	8	—	279	52.7
Bucksport	4,937	17.42	—	—	—	8	25	48	5	—	86	31.4
Mount Desert Island	2,059	15.54	—	—	—	—	5	27	—	—	32	6.3
Southwest Harbor	1,765	28.33	—	—	—	—	13	37	—	—	50	30.0
Gouldsboro	1,733	9.23	—	—	—	1	2	13	—	—	16	93.8
Swan's Island	331	39.27	—	—	—	—	5	7	1	—	13	7.7
Winter Harbor	514	11.67	—	—	—	1	1	4	—	—	6	33.3
Hancock SP	—	—	1	—	—	8	84	103	8	—	204	27.9
Hancock County Totals	54,562	17.52	2	—	4	25	260	636	29	—	956	37.2
Total Urban Areas	24,467	23.01	1	—	3	14	127	404	14	—	563	41.2
Total Rural Areas	30,095	13.06	1	—	1	11	133	232	15	—	393	31.6

<i>Kennebec County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Kennebec SO	—	—	—	11	3	9	109	169	17	1	319	25.4
Augusta	18,893	66.96	1	20	16	25	206	961	31	5	1,265	45.3
Gardiner	5,731	30.36	—	3	—	7	23	140	1	—	174	28.2
Hallowell	2,362	27.10	—	1	—	3	10	48	2	—	64	15.6
Waterville	15,897	53.34	—	15	13	15	105	684	15	1	848	38.2
Oakland	6,253	16.79	—	3	—	—	24	72	6	—	105	24.8
Monmouth	4,105	13.64	—	—	—	1	16	34	5	—	56	25.0
Winslow	7,704	20.90	—	6	2	3	33	112	5	—	161	24.2
Winthrop	6,051	22.31	—	—	1	2	36	94	2	—	135	35.6
Clinton	3,425	12.26	—	2	—	2	11	25	2	—	42	31.0
Kennebec SP	—	—	1	2	1	9	98	200	12	2	325	42.2
Kennebec County Totals	121,635	28.73	2	63	36	76	671	2,539	98	9	3,494	37.6
Total Urban Areas	70,421	40.47	1	50	32	58	464	2,170	69	6	2,850	38.5
Total Rural Areas	51,214	12.57	1	13	4	18	207	369	29	3	644	33.9

<i>Knox County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Knox SO	—	—	—	1	2	10	53	200	15	—	281	24.6
Camden	4,848	17.12	—	1	—	1	14	66	1	—	83	31.3
Rockland	7,205	34.56	—	1	—	7	31	203	7	—	249	37.8
Thomaston	2,776	22.33	—	—	—	—	7	55	—	—	62	29.0
Rockport	3,314	6.64	—	—	—	—	4	17	1	—	22	54.5
Knox SP	—	—	1	1	—	—	—	3	—	—	5	80.0
Knox County Totals	39,615	17.72	1	4	2	18	109	544	24	—	702	31.8
Total Urban Areas	18,143	22.93	—	2	—	8	56	341	9	—	416	36.1
Total Rural Areas	21,472	13.32	1	2	2	10	53	203	15	—	286	25.5

<i>Lincoln County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Lincoln SO	—	—	—	17	1	7	89	171	12	—	297	25.6
Boothbay Harbor	2,135	29.04	—	—	—	1	9	50	1	1	62	72.6
Damariscotta	2,204	16.33	—	1	—	1	1	32	—	1	36	22.2
Waldoboro	5,016	14.95	—	2	1	1	19	51	—	1	75	29.3
Wiscasset	3,673	16.61	—	2	1	5	15	37	1	—	61	26.2
Lincoln SP	—	—	—	1	—	1	1	—	—	—	3	66.7
Lincoln County Totals	34,079	15.67	—	23	3	16	134	341	14	3	534	31.6
Total Urban Areas	13,028	17.96	—	5	2	8	44	170	2	3	234	38.9
Total Rural Areas	21,051	14.25	—	18	1	8	90	171	12	—	300	26.0

<i>Oxford County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Oxford SO	—	—	—	11	1	4	118	232	5	—	371	31.8
Rumford	5,738	39.39	—	2	2	2	48	168	3	1	226	26.5
Dixfield	2,504	26.76	—	—	—	1	15	50	—	1	67	56.7
Mexico	2,633	50.13	—	2	—	1	51	75	3	—	132	20.5
Norway	4,970	29.58	—	7	—	2	27	109	2	—	147	50.3
Paris	5,140	24.12	—	—	—	2	23	95	4	—	124	29.8
Fryeburg	3,407	13.80	—	1	1	3	9	32	—	1	47	53.2
Oxford	4,075	54.48	—	1	—	3	21	193	4	—	222	40.1
Oxford SP	—	—	—	2	1	8	66	100	8	—	185	34.1
Oxford County Totals	57,327	26.53	—	26	5	26	378	1,054	29	3	1,521	34.9
Total Urban Areas	28,467	33.90	—	13	3	14	194	722	16	3	965	36.3
Total Rural Areas	28,860	19.27	—	13	2	12	184	332	13	—	556	32.6

<i>Penobscot County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Penobscot SO	—	—	—	1	6	2	176	396	17	2	600	26.3
Bangor	32,744	58.58	3	10	35	22	243	1,564	37	4	1,918	30.2
Brewer	9,376	32.53	—	—	2	5	44	251	3	—	305	40.0
Dexter	3,856	27.49	—	—	2	3	20	77	4	—	106	24.5
Lincoln	5,094	39.85	—	—	1	1	54	142	5	—	203	30.5
Old Town	7,736	21.07	1	1	2	7	22	127	3	—	163	18.4
Orono	10,663	17.72	—	1	1	1	33	152	1	—	189	25.4
Hampden	7,275	16.91	—	1	1	2	18	97	4	—	123	16.3
Millinocket	4,430	18.06	—	1	1	1	24	52	1	—	80	22.5
East Millinocket	3,027	18.83	—	—	—	—	8	49	—	—	57	19.3
Newport	3,250	30.46	—	—	2	—	12	85	—	—	99	47.5
Veazie	1,895	33.77	—	—	1	—	8	55	—	—	64	37.5
University of ME Orono	—	—	—	2	—	—	11	163	2	11	189	6.9
Holden	3,094	26.83	—	—	—	1	32	50	—	—	83	9.6
Penobscot MDEA	—	—	—	—	—	—	—	1	—	—	1	100.0
Penobscot SP	—	—	2	6	2	10	107	178	11	2	318	32.4
Penobscot County Totals	153,530	29.30	6	23	56	55	812	3,439	88	19	4,498	28.2
Total Urban Areas	92,440	38.73	4	16	48	43	529	2,865	60	15	3,580	28.2
Total Rural Areas	61,090	15.03	2	7	8	12	283	574	28	4	918	28.4

<i>Piscataquis County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Piscataquis SO	—	—	—	—	1	3	41	62	17	—	124	25.0
Dover-Foxcroft	4,110	34.55	—	—	1	8	22	103	6	2	142	16.2
Milo	2,295	43.57	—	—	—	18	21	58	3	—	100	34.0
Brownville	1,225	19.59	—	—	1	—	10	11	2	—	24	25.0
Greenville	1,624	28.33	—	—	—	4	10	31	—	1	46	37.0
Piscataquis SP	—	—	—	—	—	—	3	1	—	—	4	0.0
Piscataquis County Totals	17,191	25.59	—	—	3	33	107	266	28	3	440	25.2
Total Urban Areas	9,254	33.72	—	—	2	30	63	203	11	3	312	25.6
Total Rural Areas	7,937	16.13	—	—	1	3	44	63	17	—	128	24.2

<i>Sagadahoc County</i>		<i>January–December 2013</i>											
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate	
Sagadahoc SO	—	—	—	4	—	4	44	108	9	1	170	29.4	
Bath	8,384	36.14	—	2	1	5	26	262	2	5	303	35.0	
Topsham	8,728	18.22	—	1	1	2	27	117	10	1	159	19.5	
Richmond	3,388	6.20	—	—	—	—	5	15	1	—	21	23.8	
Phippsburg	2,230	5.38	—	—	—	—	3	9	—	—	12	0.0	
Sagadahoc SP	—	—	—	—	—	1	1	1	1	—	4	25.0	
Sagadahoc County Totals	35,145	19.04	—	7	2	12	106	512	23	7	669	28.8	
Total Urban Areas	22,730	21.78	—	3	2	7	61	403	13	6	495	28.7	
Total Rural Areas	12,415	14.02	—	4	—	5	45	109	10	1	174	29.3	

<i>Somerset County</i>		<i>January–December 2013</i>											
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate	
Somerset SO	—	—	—	9	1	10	127	242	24	2	415	24.1	
Fairfield	6,657	37.85	—	2	—	4	49	192	5	—	252	32.9	
Skowhegan	8,537	60.68	—	9	2	7	86	389	22	3	518	22.6	
Madison	4,776	22.40	—	2	—	2	21	76	6	—	107	26.2	
Pittsfield	4,162	11.53	—	—	—	—	3	41	3	1	48	81.3	
Somerset SP	—	—	1	2	1	4	32	124	8	—	172	62.8	
Somerset County Totals	51,745	29.22	1	24	4	27	318	1,064	68	6	1,512	31.4	
Total Urban Areas	24,132	38.33	—	13	2	13	159	698	36	4	925	28.9	
Total Rural Areas	27,613	21.26	1	11	2	14	159	366	32	2	587	35.4	

<i>Waldo County</i>		<i>January–December 2013</i>											
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate	
Waldo SO	—	—	—	2	—	10	84	118	11	1	226	38.5	
Belfast	6,654	24.50	1	—	—	8	29	124	1	—	163	41.7	
Searsport	2,618	24.83	—	—	—	—	17	45	3	—	65	18.5	
Islesboro	568	8.80	—	—	—	—	3	2	—	—	5	60.0	
Waldo SP	—	—	—	—	—	2	24	81	10	—	117	38.5	
Waldo County Totals	38,780	14.85	1	2	—	20	157	370	25	1	576	37.3	
Total Urban Areas	9,840	23.68	1	—	—	8	49	171	4	—	233	35.6	
Total Rural Areas	28,940	11.85	—	2	—	12	108	199	21	1	343	38.5	

<i>Washington County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
Washington SO	—	—	—	—	—	11	50	72	7	—	140	25.7
Calais	3,054	54.68	—	2	—	9	18	138	—	—	167	58.7
Eastport	1,302	14.59	—	—	—	3	6	9	1	—	19	52.6
Machias	2,173	24.39	—	1	2	5	7	37	—	1	53	43.4
Baileyville	1,487	28.24	—	—	—	10	9	22	1	—	42	57.1
Milbridge	1,340	6.72	—	—	1	1	1	6	—	—	9	55.6
Washington SP	—	—	—	—	—	11	57	64	8	—	140	40.0
Washington County Totals	32,317	17.64	—	3	3	50	148	348	17	1	570	44.2
Total Urban Areas	9,356	31.00	—	3	3	28	41	212	2	1	290	55.2
Total Rural Areas	22,961	12.19	—	—	—	22	107	136	15	—	280	32.9

<i>York County</i>		<i>January–December 2013</i>										
Contributing Agency	Estimated Population	Crime Rate	Murder	Rape	Robbery	Aggravated Assault	Burglary	Larceny	M/V Theft	Arson	Total Index Crimes	Clearance Rate
York SO	—	—	—	2	6	19	116	177	14	6	340	35.3
Biddeford	21,324	59.28	1	19	24	75	149	972	18	6	1,264	37.7
Kittery	9,540	18.87	—	6	3	2	12	153	3	1	180	45.0
Old Orchard Beach	8,681	30.53	—	5	—	4	67	183	5	1	265	12.5
Saco	18,848	28.38	—	5	8	10	133	363	12	4	535	20.6
Sanford	20,913	42.13	—	19	12	39	135	642	26	8	881	26.4
Berwick	7,529	17.67	—	3	—	5	37	84	2	2	133	33.1
Eliot	6,257	6.23	—	2	1	1	4	31	—	—	39	41.0
Kennebunk	11,023	12.79	—	1	1	5	30	102	2	—	141	41.1
Kennebunkport	3,517	18.48	—	1	—	—	17	47	—	—	65	16.9
North Berwick	4,620	7.79	—	—	—	3	14	17	1	1	36	50.0
Ogunquit	905	43.09	—	—	—	1	5	33	—	—	39	17.9
South Berwick	7,275	10.45	—	4	—	—	12	57	3	—	76	13.2
Wells	9,803	12.96	—	3	—	2	42	77	3	—	127	13.4
York	12,695	17.88	—	2	1	4	53	161	5	1	227	15.9
Buxton	8,103	13.58	—	1	—	10	25	68	5	1	110	30.9
York SP	—	—	—	1	—	26	101	118	11	—	257	26.5
York County Totals	199,400	23.65	1	74	56	206	952	3,285	110	31	4,715	29.1
Total Urban Areas	151,033	27.27	1	71	50	161	735	2,990	85	25	4,118	28.8
Total Rural Areas	48,367	12.34	—	3	6	45	217	295	25	6	597	31.5

<i>State Totals</i>												
Grand Total	1,328,302	24.21	24	359	335	943	6,453	23,006	902	140	32,162	32.2
Total Urban Areas	846,180	29.85	12	274	297	718	4,221	19,028	599	111	25,260	32.5
Total Rural Areas	482,122	14.32	12	85	38	225	2,232	3,978	303	29	6,902	31.2

POLICE EMPLOYMENT DATA

The Uniform Crime Reporting System in Maine incorporates a collection of important data relating to police within the state. Information such as ratio of police to population, assaults on officers, and related analysis are covered in this section.

As of October 31, 2013, the following information was gathered from 134 reporting agencies.

Sworn Personnel

- There were 1,594 full-time municipal law enforcement officers, representing 1.88 officers per 1,000 population for urban population areas.
- There were 348 full-time sworn law enforcement officers employed by Maine's 16 Sheriff's Departments. There were 311 sworn officers employed by the Maine State Police. The ratio of officers per 1,000 population in rural areas is 1.37.
- Statewide, there were 2,275 full-time sworn law enforcement officers. The total complement of officers represents a rate of 1.71 officers per 1,000 population.
- Nationally, in 2012, the average rate per 1,000 was 2.4. The average 2012 rate for the New England states was 2.1.

Civilian Personnel

- The number of full-time civilian support personnel employed by the municipal departments in Maine was 359.
- There were 75 civilians employed full-time by the county Sheriff's Departments. The Maine State Police employed 129 full-time civilians.
- The total number of full-time civilian support personnel employed statewide was 589.

Caution should be exercised in using rates for comparative purposes, since a wide variety of factors dictate the number of employees necessary to various law enforcement agencies. The term "full-time sworn" officers does not mean that these personnel are performing regular police enforcement duties in investigations, patrol and deterrent practices. The need for regulatory duties, correction duties, administrative duties and assigned special duties affects the number of personnel available for regular law enforcement duties. Comparing agencies should not be done without considering the "in-house" duties and responsibilities of the agencies involved.

Figures for Sheriff's Department personnel for the year 2013 do not include persons serving as correctional or court personnel in all Sheriff's Departments. Population figures given here may vary from those shown in the County Crime Analysis (pp. 98-104), which reflect a population update at another part of the year.

Police Employment Data 2013

Agency	Population	Sworn Law Enforcement Officers			Civilian Personnel		Total		Total
		M	F	Officers/ 1,000	M	F	M	F	
Androscoggin SO	27,942	19	—	0.7	6	4	25	4	29
Auburn PD	22,948	48	4	2.3	2	5	50	9	59
Lewiston PD	36,422	74	7	2.2	3	8	77	15	92
Livermore Falls PD	3,161	6	—	1.9	—	—	6	—	6
Lisbon PD	8,923	12	1	1.5	2	3	14	4	18
Mechanic Falls PD	3,013	5	—	1.7	—	—	5	—	5
Sabattus PD	5,060	6	1	1.4	—	1	6	2	8
Total Androscoggin	107,469	170	13	1.7	13	21	183	34	217
Aroostook SO	28,220	14	1	0.5	4	2	18	3	21
Caribou PD	8,012	15	—	1.9	—	1	15	1	16
Fort Fairfield PD	3,412	3	—	0.9	—	—	3	—	3
Fort Kent PD	4,055	4	—	1.0	1	3	5	3	8
Houlton PD	6,046	13	1	2.3	1	3	14	4	18
Madawaska PD	3,957	4	1	1.3	—	1	4	2	6
Presque Isle PD	9,483	14	2	1.7	1	4	15	6	21
Van Buren PD	2,125	3	—	1.4	—	—	3	—	3
Ashland PD	1,277	2	—	1.6	—	—	2	—	2
Limestone PD	2,269	3	—	1.3	—	—	3	—	3
Washburn PD	1,651	1	—	0.6	—	—	1	—	1
Total Aroostook	70,507	76	5	1.1	7	14	83	19	102
Cumberland SO	51,883	56	4	1.2	6	5	62	9	71
Brunswick PD	20,354	31	2	1.6	7	9	38	11	49
Cape Elizabeth PD	9,104	13	—	1.4	1	—	14	—	14
Falmouth PD	11,468	17	—	1.5	6	3	23	3	26
Gorham PD	16,764	22	1	1.4	—	2	22	3	25
Portland PD	66,256	139	20	2.4	14	43	153	63	216
South Portland PD	25,126	50	4	2.1	3	4	53	8	61
Scarborough PD	19,252	34	3	1.9	13	4	47	7	54
Westbrook PD	17,647	35	3	2.2	1	1	36	4	40

Agency	Population	Sworn Law Enforcement			Civilian		Total		Total
		Officers	Officers/ 1,000	Officers/ 1,000	Personnel	Personnel	M	F	
Bridgton PD	5,308	8	—	1.5	—	1	8	1	9
Cumberland PD	7,353	11	—	1.5	—	1	11	1	12
Freeport PD	8,094	12	1	1.6	—	2	12	3	15
Yarmouth PD	8,460	12	1	1.5	—	1	12	2	14
Windham PD	17,363	24	1	1.4	1	3	25	4	29
Univ. Maine - Gorham	—	10	1	—	5	3	15	4	19
Total Cumberland	284,432	474	41	1.8	57	82	531	123	654
Franklin SO	12,062	21	1	1.8	6	6	27	7	34
Farmington PD	7,657	12	1	1.7	—	1	12	2	14
Jay PD	4,827	7	—	1.5	—	1	7	1	8
Wilton PD	4,066	6	—	1.5	—	—	6	—	6
Rangeley PD	1,176	3	—	2.6	—	—	3	—	3
Univ. Maine - Farmington	—	4	—	—	—	—	4	—	4
Carrabassett Valley PD	780	2	—	2.6	—	—	2	—	2
Total Franklin	30,568	55	2	1.9	6	8	61	10	71
Hancock SO	30,095	16	—	0.5	—	2	16	2	18
Bar Harbor PD	5,275	13	—	2.5	1	3	14	3	17
Ellsworth PD	7,853	14	2	2.0	—	4	14	6	20
Bucksport PD	4,937	7	—	1.4	2	2	9	2	11
Mount Desert PD	2,059	7	—	3.4	2	2	9	2	11
Southwest Harbor PD	1,765	5	—	2.8	2	2	7	2	9
Gouldsboro PD	1,733	2	—	1.2	—	—	2	—	2
Swan's Island PD	331	1	—	3.0	—	—	1	—	1
Winter Harbor PD	514	—	—	—	—	—	—	—	0
Total Hancock	54,562	65	2	1.2	7	15	72	17	89
Kennebec SO	51,214	21	—	0.4	—	3	21	3	24
Augusta PD	18,893	37	3	2.1	7	8	44	11	55
Gardiner PD	5,731	12	—	2.1	—	1	12	1	13
Hallowell PD	2,362	2	1	1.3	—	—	2	1	3
Waterville PD	15,897	28	3	2.0	3	7	31	10	41
Oakland PD	6,253	10	—	1.6	—	1	10	1	11
Monmouth PD	4,105	4	—	1.0	—	—	4	—	4
Winslow PD	7,704	8	1	1.2	—	1	8	2	10
Winthrop PD	6,051	8	—	1.3	5	1	13	1	14
Clinton PD	3,425	2	—	0.6	—	—	2	—	2
Total Kennebec	121,635	132	8	1.2	15	22	147	30	177
Knox SO	21,472	18	2	0.9	—	1	18	3	21
Camden PD	4,848	9	1	2.1	1	1	10	2	12
Rockland PD	7,205	18	—	2.5	2	1	20	1	21
Thomaston PD	2,776	5	—	1.8	—	—	5	—	5
Rockport PD	3,314	6	—	1.8	1	—	7	—	7
Total Knox	39,615	56	3	1.5	4	3	60	6	66
Lincoln SO	21,051	24	—	1.1	—	2	24	2	26
Boothbay Harbor PD	2,135	7	—	3.3	—	1	7	1	8
Damariscotta PD	2,204	4	—	1.8	—	—	4	—	4
Waldoboro PD	5,016	7	—	1.4	—	1	7	1	8
Wiscasset PD	3,673	2	1	0.8	—	—	2	1	3
Total Lincoln	34,079	44	1	1.3	—	4	44	5	49
Oxford SO	28,860	24	2	0.9	1	1	25	3	28
Rumford PD	5,738	9	—	1.6	—	—	9	—	9
Dixfield PD	2,504	4	1	2.0	—	—	4	1	5
Mexico PD	2,633	4	1	1.9	—	—	4	1	5
Norway PD	4,970	8	—	1.6	—	1	8	1	9
Paris PD	5,140	7	—	1.4	—	1	7	1	8
Fryeburg PD	3,407	5	1	1.8	—	—	5	1	6
Oxford PD	4,075	6	—	1.5	—	1	6	1	7
Total Oxford	57,327	67	5	1.3	1	4	68	9	77
Penobscot SO	61,090	28	1	0.5	—	5	28	6	34
Bangor PD	32,744	70	4	2.3	4	9	74	13	87
Brewer PD	9,376	16	3	2.0	—	1	16	4	20
Dexter PD	3,856	5	—	1.3	—	—	5	—	5
Lincoln PD	5,094	5	1	1.2	—	1	5	2	7
Old Town PD	7,736	11	3	1.8	—	1	11	4	15
Orono PD	10,663	12	1	1.2	—	1	12	2	14

POLICE EMPLOYMENT DATA

Agency	Population	Sworn Law Enforcement			Civilian Personnel		Total		Total
		Officers	Officers/ 1,000	Officers/ 1,000	M	F	M	F	
Hampden PD	7,275	10	—	1.4	—	1	10	1	11
Millinocket PD	4,430	5	—	1.1	—	—	5	—	5
East Millinocket PD	3,027	4	—	1.3	—	—	4	—	4
Newport PD	3,250	7	—	2.2	—	—	7	—	7
Veazie PD	1,895	4	—	2.1	—	—	4	—	4
Univ. Maine - Orono	—	18	1	—	5	3	23	4	27
Holden PD	3,094	3	—	1.0	—	—	3	—	3
Total Penobscot	153,530	198	14	1.4	9	22	207	36	243
Piscataquis SO	7,937	7	—	0.9	7	3	14	3	17
Dover-Foxcroft PD	4,110	5	—	1.2	—	—	5	—	5
Milo PD	2,295	3	—	1.3	—	—	3	—	3
Brownville PD	1,225	2	—	1.6	—	—	2	—	2
Greenville PD	1,624	2	—	1.2	—	1	2	1	3
Total Piscataquis	17,191	19	—	1.1	7	4	26	4	30
Sagadahoc SO	12,415	19	—	1.5	—	2	19	2	21
Bath PD	8,384	17	1	2.1	1	3	18	4	22
Topsham PD	8,728	11	1	1.4	—	1	11	2	13
Richmond PD	3,388	4	1	1.5	—	—	4	1	5
Phippsburg PD	2,230	1	—	0.4	—	—	1	—	1
Total Sagadahoc	35,145	52	3	1.6	1	6	53	9	62
Somerset SO	27,613	15	—	0.5	—	2	15	2	17
Fairfield PD	6,657	7	1	1.2	—	1	7	2	9
Skowhegan PD	8,537	12	2	1.6	—	1	12	3	15
Madison PD	4,776	16	—	3.4	—	1	16	1	17
Pittsfield PD	4,162	6	—	1.4	—	—	6	—	6
Total Somerset	51,745	56	3	1.1	—	5	56	8	64
Waldo SO	28,940	18	—	0.6	—	2	18	2	20
Belfast PD	6,654	13	—	2.0	—	1	13	1	14
Searsport PD	2,618	3	—	1.1	—	—	3	—	3
Islesboro PD	568	1	—	1.8	—	—	1	—	1
Total Waldo	38,780	35	—	0.9	—	3	35	3	38
Washington SO	22,961	10	—	0.4	—	1	10	1	11
Calais PD	3,054	8	—	2.6	—	1	8	1	9
Eastport PD	1,302	4	—	3.1	—	—	4	—	4
Machias PD	2,173	4	—	1.8	—	—	4	—	4
Baileyville PD	1,487	3	—	2.0	—	—	3	—	3
Milbridge PD	1,340	2	—	1.5	—	—	2	—	2
Total Washington	32,317	31	—	1.0	—	2	31	2	33
York SO	48,367	27	—	0.6	1	3	28	3	31
Biddeford PD	21,324	44	2	2.2	8	14	52	16	68
Kittery PD	9,540	17	2	2.0	1	5	18	7	25
Old Orchard Beach PD	8,681	18	2	2.3	—	2	18	4	22
Saco PD	18,848	31	3	1.8	8	6	39	9	48
Sanford PD	20,913	35	4	1.9	—	4	35	8	43
Berwick PD	7,529	11	—	1.5	—	1	11	1	12
Eliot PD	6,257	7	—	1.1	—	1	7	1	8
Kennebunk PD	11,023	16	3	1.7	1	1	17	4	21
Kennebunkport PD	3,517	11	1	3.4	1	3	12	4	16
North Berwick PD	4,620	8	—	1.7	—	1	8	1	9
Ogunquit PD	905	8	1	9.9	—	2	8	3	11
South Berwick PD	7,275	8	—	1.1	1	3	9	3	12
Wells PD	9,803	18	3	2.1	4	4	22	7	29
York PD	12,695	23	2	2.0	4	6	27	8	35
Buxton PD	8,103	7	—	0.9	3	4	10	4	14
Total York	199,400	289	23	1.6	32	60	321	83	404
All Other Dept. of Pub. Sfty.	—	20	2	—	19	7	39	9	48
Maine State Police	—	287	24	—	59	70	346	94	440
Totals	1,328,302	2,126	149	1.7	237	352	2,363	501	2,864



CARIBOU POLICE DEPARTMENT

25 High Street, Suite 4
Caribou, Me 04736

(207) 493-3301
Fax: (207) 493-4201

Hauling Prisoners Overview 2012-2014

2014

Caribou PD prisoners: 127
Projected extra mileage: 15,875
Minimum overtime expense: \$20,320 (\$40.00 per hour per 4 hours overtime)
Estimated fuel: \$4,101 (average of \$3.10 a gallon)
Estimated vehicle repair: \$1,081 (\$0.0681 per mile based on AAA cost analysis of an SUV)

2013

Caribou PD prisoners: 158
Projected extra mileage: 19,750
Minimum overtime expense: \$25,280 (\$40.00 per hour per 4 hours overtime)
Estimated fuel: \$5,267 (average of \$3.20 a gallon)
Estimated vehicle repair: \$1,345 (\$0.0681 per mile based on AAA cost analysis of an SUV)

2012

Caribou PD prisoners: 171
Projected extra mileage: 21,375
Minimum overtime expense: \$27,360 (\$40.00 per hour per 4 hours overtime)
Estimated fuel: \$5,665 (average of \$3.18 a gallon)
Estimated vehicle repair: \$1,456 (\$0.0681 per mile based on AAA cost analysis of an SUV)

152 average trips
19000 average miles

\$24,320 average overtime
\$5,011 in average fuel
\$1,294 in average repairs
\$30,625 in extra expenses (average)

Would probably need to replace vehicles every 10 months versus every 12-18 months
Extra cruisers not always available due to detail enforcement

Comparison of Caribou/Presque Isle pay rates

	Step/Year 1	Step/Year 2	Step/Year 3	Step/Year 4	Step/Year 5	10 Years	17 Years
Caribou Police Officer	\$ 14.47	\$ 16.29	\$ 16.83	\$ 17.31	\$ 17.80	\$ 19.37	\$ 20.42
Presque Isle Police Officer	\$ 15.91	\$ 16.21	\$ 17.39	\$ 18.15	\$ 18.92		\$ 20.30
Presque Isle Dispatcher	\$ 14.45	\$ 14.97	\$ 15.74	\$ 16.26	\$ 16.77	\$ 18.18	



CARIBOU POLICE DEPARTMENT

25 High Street, Suite 4
Caribou, Me 04736

(207) 493-3301
Fax: (207) 493-4201

12/08/14

Sexual/child abuse case for 2014

For two thousand fourteen the Caribou Police Department has handled forty eight sexual or child abuse cases. This has been the highest number that I have seen for the Caribou Police Department since I have been employed here. These cases range from a simple assault or to the more serious crime of a child being touched inappropriately. The reason for this being the highest year is because The Department of Human Resources is backlogged with cases that have been reported to them. DHHS is now filtering their cases out to local law enforcement to help with the backlog. I don't feel that you will see these numbers go down.

Just wanted to give you the numbers from previous years.

2008	10
2009	16
2010	16
2011	19
2012	23
2013	25
2014	48

As you can see from above the numbers have been steadily climbing.

This is a breakdown of the 2014 sexual/child abuse for the annual crime report:

Unlawful Sexual Contact	20
Gross Sexual Assault	4
Other	24
<hr/>	
Total	48

Thank you
Sgt. Mark Gahagan



OFFICE OF THE CITY MANAGER
CARIBOU, MAINE

To: Mayor and Council Members
From: Austin Bless, City Manager and Scott Susi, Fire Chief
Date: February 23, 2015
Re: Utilizing Basic EMTs

Another topic brought up by the council was utilizing Basic EMT's instead of having all paramedics on staff. This is certainly possible.

Here is a comparison of wages for a Basic EMT vs Paramedic.

	BASIC EMT	PARAMEDIC
BASE	\$479.55	\$479.55
FF I/II	\$20.81	\$20.81
LICENSE	\$25.98	\$167.00
TOTAL	\$526.34 per week	\$667.36 per week

Difference \$141.02 per week or \$7,333.04 per year. If we were to replace 3 Paramedics with Basics we could save \$21,999.12.

We could replace 6 paramedics with 6 basics. That would put 2 basics on each crew with 3 paramedics. This would save \$43,998.24.

However if we switched to only having 3 paramedics on each crew we could not guarantee there would always be a paramedic available to go on a call. This would require that we drop down our ambulance license (department wide) from an ALS to a Basic License. Because ALS calls are paid at a higher rate than Basics dropping to the basic level of license means we would lose \$96 per local emergency call. We do about 1,280 local emergency calls each year which would mean a loss of \$122,880 in revenue each year.

Dropping down to the Basic Level would also mean we could not do ALS Transfers. In 2014 the ALS transfers we did added up to \$569,563.70. So switching to 6 basics would save us \$43,998.24 but result in a loss of revenue of \$692,443.70.



OFFICE OF THE CITY MANAGER
CARIBOU, MAINE

To: Mayor and Council Members
From: Austin Bleess, City Manager
Date: February 23, 2015
Re: Cary Medical Center

Another topic discussed during the budget meetings was seeing if Cary Medical Center would pay a Fee For Service to the city. As they are a department of a City they are not a non-profit, as the other organizations that have fee for service agreements with the city.

At the last joint Cary/Council meeting it was discussed the Hospital Board, which the Council appoints, is charged with overseeing the operations. The Hospital District owns and is responsible for the grounds and buildings.

The Council discussed a fee for service concept at the last meeting, however there was no resolution to that. If the Council wishes to ask Cary to enter into a similar type of agreement I would recommend a letter be sent to the Board of Directors for them to consider at their next meeting.



OFFICE OF THE CITY MANAGER
CARIBOU, MAINE

To: Mayor and Council Members
From: Austin Bless, City Manager
Date: February 23, 2015
Re: Building Permit Fees

Another topic discussed during the budget season was possibly changing the building permit fee structure.

Currently our permit fee structure is as follows:

Estimated Costs of Construction

\$1 – 9,999	\$50.00
\$10,000 – and Up	\$6.00 per \$1,000
Demolition Permit	\$25.00

This results in people providing an estimate of construction costs which may or may not be accurate in order to reduce the permit fees.

It has been brought up to me by some councilors and residents about how our permit fees are higher than some of our neighboring communities. It's been suggested that perhaps we should reduce our fee to a flat rate.

Another route would be to charge a fee per square foot. That would take away the guessing of an "estimated cost of construction".

In 2013 our expense budget for Code Enforcement was \$40,525 in 2015 it is \$26,361. The revenue budget in 2013 was \$28,340, and in 2015 is \$24,280. If we were to change our permit fees we may be able to encourage building in Caribou and we would recoup the costs over the long term by adding to the tax base.

In 2014 we issued 52 building permits and took in \$18,366 in revenue from those.

If this is a topic the Council would like staff to look into further we can do that. But there are quite a few variables that could play into this, so we wanted feedback from the Council as to whether or not this is a topic they want to look at or not.

Reducing the demolition permit fee may be merited as well. We do have to complete some report on demolition permits, but perhaps a lower permit fee would be more appropriate, especially where a person is removing slum and blight from the community.