DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS TESTIMONY BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY
Oversight: Privacy of City Data
Monday, April 24, 2017

Good afternoon Chair Vacca and the members of the NYC Council Committee on Technology. My name is Anne Roest, and I am the City's Chief Information Officer and Commissioner of the Department of Information Technology and Telecommunications (DoITT). I am joined by Mindy Tarlow, the Director of the Mayor's Office of Operations and Chief Technology Officer (CTO) Miguel Gamiño, in addition to two of my DoITT colleagues, Michael Pastor, DoITT's General Counsel, and Geoffrey Brown, the Citywide Chief Information Security Officer (CISO). Thank you for the opportunity today to testify on the privacy of City data. I commend the Committee for its timely examination of this topic.

I want to begin by articulating the values that animate our work at DoITT, and across the entire administration, with respect to data privacy. I believe, as do my colleagues beside me, that New Yorkers' private information should stay that way—private. We also believe that the City's systems and assets must stay secure, shielded from outside threats. This is what drives our work every day.

I know that the Council shares these values, and we are grateful for your collaboration on these critical fronts, particularly in a time when the actions of the federal government appear to be working against the privacy and security of New Yorkers.

I'd first like to highlight DoITT's work in this arena by focusing on our excellent Citywide Cybersecurity team, which leads the effort to protect the City's systems and assets from ever-evolving cyber threats. This administration has made a tremendous commitment to fortify the cybersecurity team in recent years, with a significant increase in investment for enhanced technology to stay ahead of these threats, and the addition of a Citywide CISO to spearhead proactive and progressive risk-management strategies. That has put the City in a better position than we've ever been on that front.

One strategy the cyber team has employed is intensifying the role of employees in the defense of our networks. We recently created a security awareness video to help employees understand the importance of using strong passwords—a simple but extremely effective way to protect our systems. We have subsequent videos in development, including one scheduled for release in May.

A second strategy recognizes phishing as a significant attack vector. Phishing is the use of emails to trick a victim into clicking a malicious link or into providing sensitive data. We've started launching test phishing emails—a standard security practice—to see how employees

respond, and subsequently perform detailed analysis and provide training for those who need it. At the same time, we are strengthening the technical defenses to our Citywide email flow.

The Cybersecurity team also establishes Citywide Information Security policies and standards, to which city agencies and their employees must adhere. These policies and standards, which we are currently updating, inform the practices of all City agencies' interactions with the public—both online and in person.

People are thinking about privacy now more than ever. With that in mind, I can detail a few more forward-thinking policies that keep New Yorkers' information secure.

Data Classification and Encryption

We are very proud of our laws and policies that promote transparency. However, much of the information collected, generated, or maintained by the City is not public record and should remain as such—including the personal information that New Yorkers provide to agencies. To that end, one of DoITT's most vital information security policies is the data classification policy, which ensures that agencies 1) appropriately categorize their information assets, and 2) apply the appropriate degree of protection to that information. This is critical because all data with a classification of "private" or "confidential" may not be stored and/or transmitted across any communication mechanism unless it is protected using approved encryption technology.

Security Assurance

Similarly, applications – whether public-facing or internally accessible – must go through a software security assurance process. This ensures that the tools that the City develops to support City functions are built in a secure fashion, and must comply with our robust policies, standards, and industry best practices. For example, the Department of Finance just released a new mobile application to either pay or dispute a parking ticket. As anyone who has had to go through that process knows, it may be necessary to enter credit card information, which must be transmitted over a secure network. The security assurance process gives New Yorkers confidence that this convenience does not require a trade-off for safety.

Electronics Disposal and Digital Media Re-Use

The proper physical storage of data, and destruction of that data when the physical vessel is no longer in use, is extremely important. That is why DoITT formulated a digital media re-use and disposal policy, requiring that all digital media—such as computers, flash drives, smartphones, or photocopiers—undergo proper data sanitization when the devices will no longer be used. With this committee's guidance, a new law has been passed to codify this policy. Taken together, the law and policy ensure that any private information that agencies store could never accidentally fall into the wrong hands.

LinkNYC Privacy Policy

These and our other Citywide information security policies are thorough and effective for City agencies, but DoITT's role in data privacy does not end there. Wherever possible, we leverage our franchises to better educate New Yorkers of their rights, while enhancing privacy protections.

Over 1.4 million residents and visitors have connected to LinkNYC, the City's first-of-its kind franchise to transform outdated payphones into state-of-the art free Wi-Fi kiosks. This is one of the few franchises that this administration negotiated from beginning to end, and it was our priority from the start to negotiate a strong, user-first privacy policy with our franchisee, CityBridge.

Just a month ago, we unveiled an update to the privacy policy that made clear that CityBridge does not, and will never, store browsing history, track the websites that Wi-Fi users visit, or share or sell data to third parties. This latest version of the privacy policy was applauded by the New York Civil Liberties Union (NYCLU) for being responsive to concerns and improving privacy protections for LinkNYC Wi-Fi users, and we are unaware of a public Wi-Fi network that has a stronger privacy policy.

The LinkNYC privacy policy, taken together with the privacy policy for Queensbridge Connected, to which the CTO will soon speak, demonstrates that the City has set the bar high for privacy considerations across the board. We look forward to continuing the discussion with this committee today.

Federal Actions

Before concluding, I'd once again like to reinforce that we share the Council's concerns about recent actions on the federal level. As you know, Congress recently passed, and the President signed, legislation that unravels essential protections of Americans' online privacy. Unfortunately, with the leadership in place in the White House, Congress, and the Federal Communications Commission (FCC), these kinds of mandates will only become more commonplace. We will continue to monitor these efforts and comment as necessary in collaboration with the CTO's office, but we also welcome your feedback and suggestions on these crucial matters.

Data privacy is an urgent consideration that the City takes very seriously. I hope my testimony has underscored that. Thank you for the opportunity to testify today, and I will now turn it over to Miguel Gamiño, the City's Chief Technology Officer, to provide more detail on broadband privacy and Internet of Things.

###

TESTIMONY OF
MINDY TARLOW, DIRECTOR
MAYOR'S OFFICE OF OPERATIONS

BEFORE THE
NEW YORK CITY COUNCIL

COMMITTEE ON TECHNOLOGY

CITY DATA PRIVACY OVERSIGHT HEARING

APRIL 24, 2017

Good afternoon Chairman Vacca, members of the Committee on Technology. My name is Mindy Tarlow, and I'm the Director of the Mayor's Office of Operations. I am here today with DoITT's Commissioner Anne Roest, Chief Technology Officer Miguel Gamiño, and two colleagues from my office: Laura Negrón, Chief Privacy Officer and General Counsel, and Tayyab Walker, Director of Enterprise Data Solutions. On behalf of the Administration and my colleagues, I would like to thank you for the opportunity to testify at this oversight hearing on City data privacy. As you know, Commissioner Roest and I appeared before this Committee last year (February 2016) regarding the City's data privacy and security practices, and share the Committee's interest in these important issues.

Then, as now, Operations remains committed to advancing important multiagency data-sharing initiatives and human subject research, with the goal of improving the quality and coordination of services delivered to all New Yorkers—while ensuring vigilant data privacy and security practices. Such efforts are in furtherance of the City's goal, set forth in OneNYC, of expanding its internal data integration capacity so that our residents receive the right resources and services at the right time, leveraging technology to streamline efficiencies. I'd like to take this opportunity to update Committee members on our efforts and advances since last year.

HHS-Connect, known today as Worker Connect, is a technology initiative established in 2008 to help improve coordination and delivery of health and human services across City agencies. Since then, this kind of work has been expanded under the Mayor's Office of Operations, as part of an overarching strategy to more efficiently and effectively address the social service needs of New Yorkers, using advances in technology—including, as one example, ACCESS NYC, a public benefits screening tool.

Operations' **Worker Connect** program remains a valuable data-matching tool and resource for facilitating interagency case management, benefits outreach, and related purposes. An Interagency Data Exchange agreement among participating agencies—and a formal business use case process—grant read-only access to limited data elements from a limited number of City agencies for program-specific purposes, subject to prior written legal approval of the agency data owner(s).

Beyond the requisite use case approvals, Worker Connect incorporates a broad array of additional protocols to help safeguard the privacy and security of client data. As examples, user training and computer log-in banners address confidentiality restrictions and citywide IT security requirements. A "terms of use" agreement, signed by agencies receiving data, memorializes the limited purposes for which data access has been authorized. Encryption and secure file transfer protocols are used to transmit data between agencies and users.

We are planning enhancements to Worker Connect's underlying technology: the Common Client Index (CCI), an algorithm-based tool that enables electronic matching of encrypted records. Planned enhancements will allow City agencies to use the CCI as a secure service to meet their electronic data-matching needs and to de-identify linked records to support cross-agency research.

Building upon the important groundwork established by the Worker Connect model, we developed and launched a **Citywide Data Integration Initiative.** This initiative is governed by a Steering Committee established by the First Deputy Mayor, which is facilitated by the Office of Operations and includes DoITT's Commissioner, the Deputy Mayor for Health and Human Services, and appointees of the First Deputy Mayor's Office. Like Worker Connect, the Citywide Data Integration Initiative advances important multiagency data-sharing work while ensuring robust privacy and security practices.

The Citywide Data Integration Initiative memorializes Administration-wide support for a "one City" approach to data, using the City's central technology platform, DataBridge. It also provides the legal privacy and data security framework and operational protocols for developing multiagency projects involving the integration of data from three or more agencies.

With our Steering Committee's support and guidance, the Administration has undertaken additional efforts to help strengthen the City's data privacy and security practices.

For example, the Administration sought a HIPAA Security Rule assessment of the DataBridge platform. This review, led by an outside consultant in cooperation with DoITT and Operations, was launched to gauge whether DataBridge and its staff were equipped with the physical, technical, and administrative resources and protocols required by law to handle personally identifiable information. Following a four-month review, it was determined that DataBridge is compliant with HIPAA Security Rule requirements.

Finally, Operations—working with the Law Department and other City colleagues with expertise in data privacy and security—has provided internal guidance for handling third party requests for information held by City agencies, to help supplement existing agency practices. Working with our City colleagues, we will develop training materials on this subject matter that will be rolled out to agencies and can be adapted for their use with employees and contracted providers, in the months ahead.

Thank you for the opportunity to share our progress today with the Committee. In closing, I want to reiterate our commitment to advancing important data integration work, leveraging innovations in the City's technical capabilities,

while protecting the privacy and security of residents' personal data, particularly for our most vulnerable populations. We believe that our comprehensive protocols and working relationships across agencies, and with the City's Law Department, enable important City work to go forward under our collaborative leadership, with vigilant and protective stewardship. We look forward to our continued conversations on this important topic, and my colleagues and I are happy to answer any questions.

Mayor's Office of Tech + Innovation

Miguel Gamiño Jr., Chief Technology Officer for the City of New York

Testimony before the City Council Committee on Technology

City Data Privacy

Oversight Hearing

April 24, 2017

Good afternoon, Chairman Vacca and members of the Technology Committee. I am Miguel Gamiño, Chief Technology Officer (CTO) for the City of New York and I also lead the Mayor's Office of Technology and Innovation. I appreciate the opportunity to speak to issues regarding data privacy, an area that I agree is of paramount importance as we continue to connect New Yorkers to the internet and harness the opportunities presented by the proliferation of the Internet of Things (IoT).

As you are aware, Mayor de Blasio has set the goal that every resident and business will have access to affordable, reliable, high-speed internet service everywhere by 2025. While our office actively works to close the digital divide and get New Yorkers online, we are also acutely aware of the emerging internet-borne threats to human rights and democracy that increased connectivity could expose. In fact, reports show that the City's most vulnerable communities are increasingly likely to experience harassment, discrimination, a loss of privacy, and barriers to civic engagement through their use of the internet.[1][2]

Like you, we are also concerned that these threats may escalate in the wake of the most recent decision by Congress and President Trump to reverse the Federal Communication Commission's internet privacy protections, which would have placed limits on how internet service providers can use sensitive personal data, including browsing history, geolocation, and financial and medical information. To access the internet and the opportunities that come with it, we need these internet service providers to connect us to websites, network our devices, complete our calls and deliver our text messages. They should not be able to exploit this gatekeeper position to collect and sell information about our consumer habits, health conditions and political views, especially without even letting us know what they are doing. Yet this is precisely what the federal government has just enabled.

---

[1] Data and Society Research Institute and Center for Innovative Public Health Research. *Online Harassment, Digital Abuse, and Cyberstalking In America.* 11/21/16
https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

[2] Pew Research Center. *Americans and Cybersecurity.* 1/26/17
http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Despite these threats, the answer is not to shy away from the promotion of internet adoption, but rather to double down on our efforts to safeguard and empower our communities. That is why this administration has always taken seriously the need to implement measures to help protect New Yorkers, particularly vulnerable populations, through the formulation and enforcement of strict privacy policies, vigorous advocacy on federal policy and broad outreach to educate the public on best practices around internet privacy and health.

As we recently consolidated broadband oversight within the Mayor's Office of Technology and Innovation, we worked with the Counsel to the Mayor to initiate a comprehensive legal review of the City's authority to protect New Yorkers' privacy when connected to the internet. Specifically, this review includes an evaluation of the authority the City may have over the privacy policies of internet service providers; how and to what extent the City is exercising this authority currently; and whether the City can expand the exercise of its available authority to achieve, at minimum, the privacy protections for internet service consumers that Congress and the President recently repealed.

Projects such as Queensbridge Connected, which will bring free high-speed broadband to over 7,000 NYCHA residents, show the potential for the City taking a strong role in setting the terms of internet service for New Yorkers. In particular, we would highlight that the policy for Queensbridge is communicated in a clear and concise manner and restricts the transfer of personal information to third parties including the City. As was mentioned in Commissioner Roest's update on LinkNYC, we believe these policies set a high bar for privacy and we will always look to improve upon them and expand best practices to other projects.

I am also joining with the Commissioner of the New York City Commission on Human Rights to convene inter-agency working group on Internet Health and Human Rights, which will be a first-of-its-kind for municipalities looking for new methods to educate and empower their residents. The working group will review broadband programs to advise on how to ensure New Yorkers' privacy, security, and basic human rights are preserved when they go online.

Public education is also essential in order to equip residents and organizations with information they need to protect themselves. That is why are working closely with the city's public libraries to address the evolving digital literacy needs of New York City residents through training courses and informal responses to their questions. The City with Brooklyn Public Library, New York Public Library and Queens Library will set a goal that every library branch will be equipped to respond to patron inquiries related to protecting their digital privacy and security.

The City is collaborating with the Mozilla Foundation on a groundbreaking effort to create a digital security training program for city-contracted community-based organizations that serve vulnerable populations. These workshops will be tailored to fit the unique needs of the participating organizations, with the overall mission of developing standards and procedures for managing data and addressing evolving threats to digital security. The ultimate goal is to produce a scalable framework, and the Nonprofit Resiliency Committee will provide additional guidance on how this model could apply in service to all New Yorkers.

Lastly, before closing, I also want to speak to important efforts that are underway to help prepare for, and manage, the proliferation of connected devices commonly referred to as the Internet of Things or IoT. By 2020, it is estimated that the number of connected devices will exceed 50 billion. When used effectively, these devices – like sensors that capture pollution in the air or lights that only turn on when someone is in the room – can produce cost savings, bolster civic engagement, and strengthen public health and safety. They can also carry significant challenges and risks for cities, particularly in the area of privacy and data security.

To help City agencies prepare for the introduction of new technologies and mitigate potential risks, in 2015, the Mayor's Office of Technology and Innovation kicked off an extensive effort to develop a first-of-its-kind set of guidelines for the Internet of Things. The guidelines incorporate best practices from more than 50 cities around the world as well as input from subject matter experts representing universities, regulatory and standards bodies, public interest groups, and private companies. Since the release of these guidelines in May 2016, more than 40 cities around the world have followed New York City's lead and committed to a common set of guiding principles for the responsible and equitable use of IoT technologies.

The guidelines are designed to provide practical advice for agencies as they explore and consider adopting new IoT technologies, while also reinforcing existing City policies and laws around cybersecurity, data classification, and open data. Building on these guidelines, staff at the Mayor's Office of Technology and Innovation are also available to assist agencies in this process – providing subject matter expertise and a center of excellence on best practices and lessons learned related to IoT. Lastly, in March, our office announced that Brownsville, Brooklyn will be home to the City's first Neighborhood Innovation Lab. Through this unique public-private partnership, City agencies will be able to partner directly with community residents and technology companies to demonstrate and test smart city devices within these communities, gathering community feedback every step of the way.

Although much work remains to be done in our effort to more connect New Yorkers to the internet and harness the opportunities presented by the proliferation of IoT, I could not be more pleased with the pace of progress and the incredible leadership team at DoITT, The Mayor's Office of Operations and across the City. We will remain diligent in our efforts to protect the privacy of New Yorkers and appreciate the City Council's continued support in this important area.

The Internet Association

Good afternoon Chairman Vacca and distinguished members of the City Council Committee on Technology. My name is John Olsen and I am the New York Executive Director for the Internet Association (IA). Internet Association is the unified voice of the internet economy, representing interests of leading Internet companies and their global community of users. It is dedicated to advancing public policy solutions that foster innovation, promote economic growth, and empower people through the free and open Internet.

IA has established an office in New York State to provide knowledge and guidance to public policymakers on matters including privacy, cybersecurity, and data storage and processing. Association members service nearly every resident of New York City either through the Internet, such as through apps on mobile devices or daily visits to member websites, thanks in large part to cloud computing. Moreover, several of IA's members offer cloud solution services to make governments, business, and consumers' lives run more securely and efficiently.

I am here before you today to comment on the storage, use, and disposal of data and how cloud computing services increase efficiencies with respect to all three of these aspects. Cloud computing has been embraced by governments large and small. Most notably, the federal government has seen a dramatic uptick in agencies moving to cloud-based services since President Obama's "cloud first" directive issued in 2011. Government agencies with high-level security needs such as US military and intelligence services, health care agencies, and scientific research missions have moved to cloud computing, and in so doing, have greatly improved the security of their IT and increased their agility in responding to global challenges. Cities like Atlanta, Chicago, Seattle, and San Francisco have also move to cloud-based solutions to improve government functions, reduce waste, conserve energy, and quickly respond to the needs of their workforces and citizens. Some New York City agencies have also begun to leverage cloud computing to begin to deliver new and innovative services across the entire city.

Despite these first few steps forward, there is huge, untapped potential for New York City to benefit from harnessing the power of cloud. That is because cloud offers greater flexibility when it comes to scaling operations as opposed to traditional on-site data servers and maintenance. All infrastructure is maintained off-site in secure locations, and IT departments are able to devote resources and cost to increasing bandwidth, updating technologies, and building great applications. Reducing overhead allows governments to devote capital to improving operations and creates greater efficiency in the workforce.

Cloud services offer increased access to data and allow massive amounts of information to be stored and analyzed. Health records, criminal records, vehicle registrations, etc. are all available at your fingertips with cloud. In addition, data analytics help identify fraud, waste, and abuse in government systems, further increasing cost savings to municipalities. With cloud, essential data is identified quickly and unnecessary information can be quickly and securely disposed.

With an eye toward security specifically, cloud service providers offer systemic superiority when it comes to keeping private data secure. There are several key points that enforce this concept:

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.Internet Association.org

1. Cloud provides a deep integration of compliance and security with adherence to strict industry and regulatory standards and extra security tools like encryption and access management for customers;
2. Cloud providers handle much of the "surface area" by maintaining and securing the physical infrastructure – customers like government agencies can focus security personnel on more important tasks such as monitoring the applications used for unauthorized access to storage and processing;
3. The cloud offers greater visibility and access to data – security and log data can be analyzed for vulnerabilities and any weaknesses quickly remediated;
4. Cloud platforms surround traditional IT systems and provide greater insight into the behavior and function of those systems – this includes security issues and creates "defense in depth;" and
5. Economies of scale allow for greater savings with cloud in respect to massive amounts of data and the security personnel required to maintain that data.

As state and local governments are consistently being asked to do more with less, cloud computing offers an elegant and cost-effective solution to securely storing data and harnessing it for new emerging technologies like data analytics. A city like New York which serves millions of people daily could greatly benefit from a cloud first approach to its IT decision-making. The ease of use and accessibility of cloud allow 21st century governments to be more responsive to their citizens, while at the same time improving services through data analytics and reducing use of taxpayer dollars on duplicative or wasteful programs.

I thank you for your time today and would be happy to answer any questions you may have.

John Olsen
Executive Director
Internet Association – New York State

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 5799

☐ in favor ☐ in opposition

Date: 4/24/2017

(PLEASE PRINT)

Name: Anne Roest

Address: 28 Cambridge Place Brooklyn

I represent: DOITT

Address: 255 Greenwich Manhattan

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: John Olsen

Address: 111 Washington Ave Albany NY 12210

I represent: NYS Internet Association

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: STORY BELLOWS

Address: 10 GRAND ARMY PLAZA BKLYN

I represent: BROOKLYN PUBLIC LIBRARY

Address: 10 GRAND ARMY PLAZA BKLYN

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 4/24

(PLEASE PRINT)

Name: Thomas Kambar

Address: 168 7th St. Brklyn

I represent: OATS

Address: San F.

Support Q3,A w/ Mindy Tarlow

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 5799

☐ in favor ☐ in opposition

Date: 4/24/17

(PLEASE PRINT)

Name: Tayyab Walker

Address: 4 MTC, 19th Fl

I represent: Mayor's Office of Operations

Address: 253 Bway

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 5799

☐ in favor ☐ in opposition

Date: Apr. 24

(PLEASE PRINT)

Name: Mindy Tarlow

Address: Operations

I represent: _____

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 4/24/2017

(PLEASE PRINT)

Name: MIGUEL GAMINO

Address: 15 METROTECH 19TH BROOKLYN NY 11201

I represent: (CTO) MAYORS OFFICE TECH + INNOVATION

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

If needed for Q+A - M. Tarlow

Appearance Card

5799

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: 4/24/17

(PLEASE PRINT)

Name: Laura Negron

Address: NYC Mayors Office, Operations

I represent: _____

Address: _____

Please complete this card and return to the Sergeant-at-Arms

QUESTIONS IF needed, DOITT

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 5799

☐ in favor ☐ in opposition

Date: 24 APR 2017

(PLEASE PRINT)

Name: GEOFFREY BROWN

Address: 2 metrotech center, 5th FL, BROOKLYN

I represent: DOITT

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 5799

☐ in favor ☐ in opposition

Date: 4/24/17

(PLEASE PRINT)

Name: MARTHA PINTUR GENERAL COUNSEL

Address: DOITT

I represent: DOITT

Address: 2 Metro Tech, 5th FL

Please complete this card and return to the Sergeant-at-Arms